ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

ESTUDO TÉCNICO PRELIMINAR

INFORMAÇÕES BÁSICAS

Número do processo: 8515550-95.2025.8.06.0000

Código contratação: AQSETIN2025003

Área da Demanda: Coordenadoria de Nuvem e Monitoramento

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no DOD/DFD, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar a decisão de atendimento.

1. DESCRIÇÃO DA NECESSIDADE

1.1. DESCRIÇÃO DA NECESSIDADE DE NEGÓCIO

1.1.1. Diante da política de planejamento, asseguradas no Plano de Contratações de STIC, no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), além do Planejamento Estratégico Institucional, alinhada com a Estratégia Nacional do Poder Judiciário e Estratégia Nacional de TIC (ENTIC-JUD), com o objetivo de "Promover a celeridade e a qualidade na prestação dos serviços" e "Fortalecer a inteligência de dados e a cibersegurança" sem comprometer o abastecimento das unidades administrativas e judiciárias, nem mesmo deixa-las obsoletas, faz-se necessário avaliar a necessidade de aprimoramento da infraestrutura relacionados ao DOD/DFD que provocou estes estudos preliminares, a fim de evitar falta ou excesso e desperdício de bens ou serviços.

1.1.2. Neste sentido, primeiramente foram avaliadas as efetivas necessidades que justificam a provisão da demanda, conforme indicado no DOD/DFD, de substituição dos equipamentos Citrix NetScaler, cuja proximidade do fim do ciclo de vida e ausência de contrato de suporte ativo comprometem a disponibilidade e a segurança dos serviços.

1.1.3. Resta evidenciada a necessidade de uma nova solução que assegure a distribuição de tráfego, otimização de performance e proteção contra ataques cibernéticos, preservando a disponibilidade e a confiabilidade das aplicações e serviços digitais. Para tanto, exige-se uma tecnologia atualizada, com suporte técnico especializado e recursos avançados de segurança.

1.1.4. Importante, para definir a solução que atenda à necessidade efetiva que sustenta a demanda, essencialmente caracterizada como uma solução de balanceamento de carga (ADC) e firewall de aplicações web (WAF), que sejam aprofundados os seguintes aspectos:

1.1.4.1. Periodicidade da necessidade: contínua (24/7) devido ao caráter crítico da disponibilidade das aplicações.

1.1.4.2. Locais de aplicação/execução/recebimento: Datacenter do TJCE e Fórum Clóvis Beviláqua.

1.1.4.3. Unidade de medida de consumo/realização: RPS (requisições/s), throughput (Gbps), número de IPs virtuais e número de FQDNs.

1.1.4.4. Volume/quantidade requerida: RPS médio 2.000; pico 4.000 RPS; throughput médio 1 Gbps; picos 4 Gbps; número de IPs virtuais 602; número de aplicações 174 e número de FQDNs 255.

1.1.4.5. Demandantes e usuários finais: A Gerência de Cibersegurança e Ambientes Tecnológicos e o Tribunal como um todo — usuários internos (servidores, magistrados e colaboradores) e externos (cidadãos, partes, advogados) que utilizam os sistemas do TJ; impacto direto sobre a continuidade e disponibilidade dos serviços digitais.

1.2. DEMAIS REQUISITOS NECESSÁRIOS À ESCOLHA DA SOLUÇÃO

1.2.1. Este subtópico consolida os requisitos adicionais que devem ser considerados na seleção da solução de balanceamento de carga (ADC) e firewall de aplicações web (WAF), incluindo os aspectos relacionados à garantia e continuidade operacional.

1.2.2. A seguir, apresenta-se a Tabela de Rastreabilidade dos Requisitos de Negócio (RN), estruturando as necessidades identificadas, de forma a assegurar clareza e rastreabilidade no processo de contratação.

Tabela 1 - Tabela de Rastreabilidade dos Requisitos de Negócio (RN)

RN-ID	Necessidade de Negócio	Detalhamento Funcional / Requisitos Associados
RN-01	Desempenho	Capacidade de processar grandes volumes de requisições simultâneas, garantindo baixa latência e resposta ágil.
RN-02	Escalabilidade	Permitir crescimento gradual, tanto horizontal quanto vertical, acompanhando a evolução da demanda e novas aplicações.
RN-03	Segurança e Mitigação de Ameaças	Funcionalidades avançadas de proteção, incluindo mitigação de ataques distribuídos (DDoS), prevenção contra OWASP Top 10, proteção contra bots, reputação de IPs e segurança específica para APIs.
RN-04	Compatibilidade com Ambientes Híbridos	Operação integrada com aplicações hospedadas localmente (on-premises) e em nuvem, mantendo interoperabilidade e padronização com a infraestrutura atual e futura do TJCE.
RN-05	Conformidade com normativos	Atendimento às diretrizes do CNJ, LGPD e normas internas de segurança da informação e governança de TIC. Pontuar no iGovTIC para fins de alcance do nível de excelência e aumento de pontuação no item do Prêmio CNJ de Qualidade.
RN-06	Operação e Suporte	Alinhamento à capacidade interna de operação, manutenção e suporte 24x7, com SLAs rigorosos, relatórios mensais de desempenho e suporte especializado do fornecedor.
RN-07	Integração com Sistemas Existentes	Compatibilidade e integração transparente com as aplicações atuais do TJCE, incluindo sistemas judiciais, administrativos e APIs externas.
RN-08	Necessidade de Garantia	Garantia contratual para software e serviços, incluindo atualizações automáticas, suporte contínuo durante a vigência do contrato e manutenção preventiva e corretiva.

1.2.3. Havendo o atendimento desta demanda, o TJCE contará com uma infraestrutura moderna, segura e resiliente, que garantirá a continuidade dos serviços digitais com alta performance e proteção contra ameaças cibernéticas. Enfatizando que, caso contrário, ocorreria o risco de interrupções, vulnerabilidades e degradação da qualidade dos serviços prestados, o que poderia afetar até mesmo a disponibilidade das aplicações críticas, impactando diretamente a atividade fim do Tribunal.

1.3. DESCRIÇÃO DA NECESSIDADE TECNOLÓGICA

1.3.1. Atualmente, o TJCE é atendido por meio de equipamentos Citrix NetScaler, adquiridos no Contrato nº 22/2018. A solução Citrix NetScaler é implementada por meio de dispositivos físicos dedicados, responsáveis tanto pelo balanceamento de carga quanto pela proteção contra ameaças, e é composta por:

1.3.1.1. 2 (dois) equipamentos Citrix NetScaler SDX 8920HB SE Hardware (6x10/100/1000 e 4x10GE BASE-X SFP+);

1.3.1.2. 4 (quatro) módulos SFP 10 Gigabit Ethernet Short Range 300m;

1.3.1.3. 2 (dois) módulos de alimentação Power Supply, 450W AC (série 8900);

1.3.1.4. Licenciamento Platinum para os equipamentos NetScaler Management and Analytics System (MAS).

1.3.2. Considera-se que o fim do suporte do fabricante e o fim da vida útil do hardware ocorrerão em 01/04/2028, conforme indicado pela Citrix: https://support.citrix.com/s/article/CTX465183-nsc-citrix-adc-mpx-89058905z-mpxsdx-8910sdx-8910z-mpxsdx-89208920z-mpxsdx-89308930z.

Citrix Systems, Inc. announces a Notice of Status Change for the Citrix ADC (NetScaler) MPX 8905/8905Z, MPX/SDX 8910/SDX 8910Z, MPX/SDX 8920/8920Z, MPX/SDX 8930/8930Z

The tables below explain the Citrix ADC life cycle management milestones as well as important information regarding dates and options during this period. The dates and milestones provided are in accordance with stated End of Life/End of Support policies for Citrix Systems, Inc.

Table 1. Milestones and Dates for these models

Milestone	Definition	Date
Notice of Change (NSC)	The NSC date is the date on which Citrix announces the intent to initiate the lifecycle management process for a hardware platform.	1st October '22
End of Sale (EOS)	The date on which Citrix will no longer offer the product.	1st April '23
End of Maintenance (EOM)	The date for end of Software Support and Development.	1st April '28
End of Life date (EOL)	The EOL milestone signals the point at which no support or maintenance is provided. Product information will be limited to the historical material available on MyCitrix.com or other online resources and is subject to removal beyond this date.	1st April '28

Figura 1 - Aviso de fim do ciclo de vida dos equipamentos Citrix ADC (NetScaler)

1.3.3. Embora os equipamentos ainda estejam dentro do período de vida útil — com fim previsto para 01/04/2028 — atualmente não há contrato de manutenção ativo que garanta suporte técnico continuado e oficial do fabricante. Considerando que todo o tráfego do Tribunal é direcionado para esses dispositivos, torna-se estratégico planejar uma solução que garanta a continuidade dessa funcionalidade, essencial para manter a operação, a resiliência e a segurança das aplicações web. Nesse contexto, a ausência de suporte adequado acarreta uma série de riscos e limitações, de modo que:

1.3.3.1. A falta de um contrato de manutenção ativo inviabiliza o suporte adequado para resolução de falhas críticas e melhorias no ambiente.

1.3.3.2. A ausência de atualizações prejudica a capacidade de defesa contra novas ameaças e impede a correção de vulnerabilidades presentes no firmware do equipamento.

1.3.3.3. A limitação de desempenho impacta a escalabilidade e a performance das aplicações.

1.3.3.4. A falta de compatibilidade com tecnologias modernas impede a evolução da infraestrutura, como no caso da Integração Contínua e Entrega Contínua (Continuous Integration e Continuous Delivery – CI/CD).

1.3.4. O crescimento da utilização de serviços digitais e a migração progressiva de aplicações para a nuvem aumentaram a superfície de exposição do Tribunal a riscos cibernéticos. Nesse cenário, torna-se indispensável adotar uma solução de proteção moderna, capaz de oferecer: inspeção avançada de tráfego, mitigação contra-ataques DDoS, proteção contra vulnerabilidades do OWASP Top 10, segurança para APIs, defesa contra bots, alta disponibilidade e compatibilidade com ambientes híbridos

1.3.5. O Processo Administrativo nº 8517531-24.2024.8.06.0000, que trata da estratégia de modernização da infraestrutura tecnológica do TJCE, já prevê que mais de 60% do tráfego institucional será migrado para a nuvem. Esse movimento reforça a necessidade de que a solução WAAP seja projetada para operar de forma distribuída, sem depender do redirecionamento obrigatório de tráfego para o Datacenter local, garantindo baixa latência, disponibilidade contínua e proteção uniforme em ambientes híbridos (on-premise e cloud).

1.3.5.1 Embora exista previsão de expansão do uso de serviços em nuvem, parcela relevante das aplicações institucionais continuará hospedada no datacenter do TJCE, especialmente sistemas administrativos e aplicações internas acessadas por meio da rede MPLS institucional. Esse tráfego interno não é direcionado à internet e, portanto, não pode ser processado por soluções baseadas exclusivamente em nuvem sem introduzir latência adicional e dependência de conectividade externa. Dessa forma, permanece necessária uma infraestrutura local capaz de realizar a distribuição de tráfego e a terminação de conexões seguras para aplicações hospedadas no ambiente on-premises.

1.3.6. Em consonância com a Resolução CNJ nº 370, de 28 de janeiro de 2021, que em seu Art. 35 recomenda a utilização de serviços em nuvem capazes de simplificar a estrutura física, viabilizar a integração e assegurar requisitos aceitáveis de segurança da informação, proteção de dados, disponibilidade e padronização tecnológica no Poder Judiciário, a necessidade tecnológica do TJCE para adoção de solução WAF/WAAP fundamenta-se justamente na ampliação da proteção de aplicações web e APIs críticas em ambiente híbrido. A solução buscada deve não apenas substituir os recursos limitados atualmente prestados por appliances físicos, mas também alinhar-se às diretrizes nacionais de modernização, priorizando arquitetura em nuvem para garantir resiliência, escalabilidade e conformidade normativa, em especial no que se refere à continuidade dos serviços digitais e à proteção de informações sensíveis processadas pelo Tribunal.

1.3.7. Registra-se, adicionalmente, que a adoção de solução em nuvem para proteção de aplicações e APIs está em consonância com as diretrizes estabelecidas pelo Conselho Nacional de Justiça, que prevê no Índice de Governança de TIC do Poder Judiciário (iGovTIC-JUD 2024) infraestrutura tecnológica e serviços em nuvem como domínio avaliado no diagnóstico. Esse parâmetro contribui diretamente para a evolução da maturidade digital do TJCE e fortalece os indicadores de governança avaliados nacionalmente.

1.3.8. Deve-se observar ainda, como boa prática, mesmo que não aplicável de forma direta ao Poder Judiciário, a previsão da Instrução Normativa SGD/ME nº 1/2019, do Governo Federal. O item 4.1 do Anexo I dispõe que: "Os órgãos e entidades que necessitem criar, ampliar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem, salvo quando demonstrada a inviabilidade em estudo técnico preliminar da contratação". A menção a essa norma reforça a orientação estratégica do Governo Digital no sentido de privilegiar soluções baseadas em nuvem, ressalvadas situações devidamente justificadas.

1.3.9. A necessidade tecnológica do TJCE está centrada em assegurar que aplicações críticas, serviços digitais e APIs expostas ao público e a sistemas parceiros recebam proteção contínua e inteligente, alinhada às melhores práticas de mercado e aos normativos do CNJ e da LGPD. Dessa forma, considerando o contexto atual do ambiente tecnológico e as limitações identificadas, torna-se imprescindível definir um conjunto de requisitos que garantam o atendimento adequado da demanda, alinhado aos principais aspectos funcionais e técnicos que deverão orientar o processo de contratação, conforme listados a seguir:

Tabela 2 - Tabela de Rastreabilidade dos Requisitos Técnicos (RT)

RT-ID	Requisito Técnico (RT)	Detalhamento / Especificação Técnica	RN Relacionado
RT-01	Controlador de Entrega de Aplicações Web (ADC)	Função de balanceador de carga, processando alto volume de requisições, baixa latência, terminação SSL/TLS, distribuição de tráfego otimizada.	RN-01
RT-02	Firewall de Aplicação Web (WAF)	proteção contra ataques OWASP Top 10, DDoS, análise em tempo real, operação permissiva e restritiva.	RN-03 RN-05
RT-03	Escalabilidade	Expansão horizontal e vertical do poder de processamento conforme crescimento da demanda.	RN-02
RT-04	Alta Disponibilidade (HA)	Arquitetura ativa-standby, failover automático, GSLB, redundância geográfica e continuidade operacional.	RN-01 RN-03
RT-05	Treinamento Especializado	Treinamento remoto para capacitação da equipe técnica em operação, configuração e suporte.	RN-06
RT-06	Serviço de Instalação e Suporte 24x7	Instalação completa, suporte contínuo, SLA rigoroso e canais de comunicação dedicados.	RN-06 RN-08
RT-07	Conformidade Normativa (DNSSEC)	Atendimento à Resolução CNJ nº 45/2007, compatibilidade com ".jus.br", segurança e disponibilidade do serviço de DNS, incluindo iGovTIC-JUD 2024, à LGPD e a boas práticas de governança de TIC. Observância, como referência, da IN SGD/ME nº 1/2019, que orienta a priorização de soluções em nuvem para novas contratações de infraestrutura.	RN-05
RT-08	Compatibilidade com Ambientes Híbridos	Integração transparente com infraestrutura on-premises e nuvem, alta performance e segurança em ambos os ambientes.	RN-04 RN-07
RT-09	Baixa Latência	Entrega rápida de aplicações mesmo em alta demanda, uso de CDN e aceleradores de hardware dedicados.	RN-01 RN-02
RT-10	Mitigação de Robôs Automatizados (Anti-Bot)	Detecção e bloqueio de acessos automatizados maliciosos, diferenciação de tráfego legítimo e nocivo.	RN-03 RN-05
RT-11	Proteção de APIs	Segurança dedicada para APIs, incluindo autenticação, validação de payload, rate limiting e prevenção de exploração de vulnerabilidades.	RN-03 RN-07

2. ANÁLISE DE SOLUÇÕES ANTERIORES

2.1. Esta demanda não é inédita e já foi atendida por meio dos Contratos nº 22/2018 e nº 24/2023. A análise das contratações havidas fez com que a Equipe de Planejamento formasse convicção de que existem melhorias a serem apropriadas, especialmente nos seguintes aspectos:

2.1.1. Tempo de cobertura de garantia: No contrato nº 22/2018, a garantia, o suporte e a assistência técnica da solução se encerraram em 07 de agosto de 2021. Um novo Contrato nº 24/2023 foi assinado em junho de 2023, com vigência até maio de 2024, sem prorrogação, o que resultou em um período sem cobertura contratual.

2.1.2. Evolução tecnológica: A prestação de serviços especializados para suporte técnico, manutenção preventiva e corretiva mostrou necessidade de evolução tecnológica de servidores, principalmente no que tange os requisitos de segurança. A experiência com o último contrato de manutenção reforçou a importância de incorporar de forma contínua melhorias e atualizações tecnológicas à solução contratada.

2.1.3. Custo operacional: O valor global do Contrato nº 24/2023 é de R$ 348.513,42, com valor mensal de R$ 29.042,00, para o período de junho de 2023 a maio de 2024. Esse contrato possibilitou a apuração dos custos dos serviços prestados, servindo de base para análises posteriores em comparativos de TCO com outras soluções.

3. FORMAS DE ATENDIMENTO DA NECESSIDADE

3.1. Diante das particularidades da necessidade identificada, além das informações técnicas obtidas, foram consideradas, para a solução da necessidade, os seguintes meios:

3.1.1. **Aquisição de solução disponível no mercado**: Aquisição de solução disponível no mercado, fornecida como appliance físico dedicado, incluindo o hardware e os direitos de uso do software embarcado necessários à sua operação.

3.1.2. **Software as a Service (SaaS)**: Levantamento de soluções em nuvem (cloud-native) ou híbridas, considerando eventual transição para ambientes parcialmente ou totalmente em nuvem, eliminando a necessidade de aquisição e manutenção de infraestrutura física local, assegura escalabilidade sob demanda, atualizações automáticas de segurança e operação distribuída em múltiplas regiões, reduzindo latência e pontos únicos de falha.

3.2. Analisadas as possíveis formas de solução para o atendimento interno da demanda, foram também promovidas medidas e consideradas outras opções de suprimento da demanda, tais como:

3.2.1. **Software Livre:** Consideração de soluções baseadas em software livre, que ofereçam funcionalidades equivalentes de balanceamento de carga e segurança, como HAProxy, NGINX ou outros, com suporte interno ou de comunidade.

3.2.2. **Netscaler**: Manutenção dos equipamentos Citrix NetScaler atuais, com aquisição de suporte técnico estendido, aproveitando investimentos já realizados e assegura a continuidade operacional.

3.3. Ao final da análise, evidenciou-se que a necessidade de atendimento da demanda relacionada a mecanismos de controle de entrega de aplicações (ADC) e firewall de aplicações web (WAF), deve considerar aspectos de desempenho, segurança, escalabilidade e custo-benefício, em alinhamento com a estratégia de evolução tecnológica da infraestrutura de TI. Nesse sentido, a definição da solução mais adequada é realizada na etapa de Análise de Soluções Possíveis (item 5), com base em critérios objetivos como desempenho, escalabilidade, segurança, suporte técnico, custo total de propriedade (TCO) e aderência às demandas específicas do ambiente atual.

4. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

4.1. A necessidade em foco destes estudos tem o condão de combinar-se à estratégia de fortalecimento da segurança da informação e da disponibilidade de serviços digitais do TJCE, de modo que, em conjunto, signifique o pleno atendimento às demandas de proteção contra ataques cibernéticos, balanceamento de carga, escalabilidade e alta disponibilidade, garantindo a continuidade operacional, a conformidade com padrões normativos e a aderência às diretrizes de transformação digital do Poder Judiciário.

4.2. Contexto do cenário atual: A análise do ambiente atual revela a existência de um equipamento appliance físico, instalado no datacenter do TJCE, cuja função majoritária é de balanceador de carga/controlador de entrega de aplicações (ADC). O WAF opera como funcionalidade embarcada nesse mesmo appliance, não sendo uma solução WAF dedicada. Mediante esse cenário, os requisitos técnicos podem ser agrupados em três blocos: (i) requisitos específicos para ADC; (ii) requisitos específicos para WAF; e (iii) requisitos comuns aplicáveis a ambas as funcionalidades.

4.2.1 Além do tráfego proveniente da internet, parte significativa do acesso às aplicações institucionais ocorre por meio da rede MPLS corporativa, utilizada pelas unidades administrativas e judiciárias distribuídas geograficamente. Esse tráfego é direcionado diretamente ao datacenter institucional e não passa pela internet pública, razão pela qual não pode ser tratado por serviços de proteção em nuvem. Nesse contexto, a presença de um controlador de entrega de aplicações (ADC) no ambiente on-premises continua sendo necessária para processar e distribuir o tráfego interno, garantindo baixa latência, integração direta com a infraestrutura de rede e controle sobre as aplicações hospedadas localmente.

4.3. A proposta contempla a adoção de uma solução organizada por dois componentes (ou blocos funcionais), entendidos abaixo com separação clara entre funcionalidades ADC, WAF e requisitos comuns:

4.3.1. **Bloco ADC**: O Controlador de Entrega de Aplicações (ADC) deverá desempenhar a função de balanceador de carga, capaz de processar grandes volumes de requisições simultâneas, garantindo otimização do tráfego e respostas ágeis aos usuários. A solução ADC deve suportar terminação de conexões SSL/TLS, compatibilidade com a infraestrutura de certificados do Tribunal e oferecer mecanismos que preservem baixa latência na entrega de aplicações (**RT-01**).

4.3.2. **Bloco WAF**: O firewall de aplicações web (**WAF**) deverá prover proteção avançada a aplicações web, incluindo detecção por assinaturas, modos de operação permissivo e restritivo e mitigação de vulnerabilidades do OWASP Top 10 com análise em tempo real (**RT-02**). A solução WAF precisa ser escalável (horizontal e vertical) para manter eficácia de inspeção conforme o crescimento do tráfego (**RT-03**), oferecer suporte a DNSSEC conforme Resolução CNJ nº 45/2007 (**RT-07**) e operar de forma integrada em ambientes on-premises e em nuvem (**RT-08**). Deve ainda garantir baixa latência adicional na inspeção das requisições (**RT-09**), incorporar mecanismos de mitigação de bots (**RT-10**) e apresentar controles específicos para proteção de APIs (limitação de taxa, validação de payload e políticas de autenticação) (**RT-11**).

4.3.3. **Requisitos comuns**: Requisitos de contrato/serviço aplicáveis a ambos os blocos: Ambos os blocos deverão ser cobertos por programa de capacitação (treinamento) que atenda a equipe técnica (**RT-05**) e por serviço especializado que inclua instalação assistida e suporte contínuo 24x7 (**RT-06**). Em termos de disponibilidade, ambos devem contar com arquitetura de alta disponibilidade e mecanismos de failover automático que preservem sessões em andamento; recomenda-se também suporte a GSLB quando aplicável para distribuição geográfica do tráfego e recuperação de desastre (**RT-04**).

4.4. Esses requisitos podem ser ofertados de forma integrada em uma única solução ou distribuídos entre soluções distintas. Assim, o conjunto proposto se alinha aos princípios da eficiência e da continuidade do serviço público, promovendo a sustentação da infraestrutura crítica de Tecnologia da Informação que dá suporte direto às atividades jurisdicionais, administrativas e de atendimento do TJCE, em consonância com as diretrizes de transformação digital do Poder Judiciário e com os normativos do CNJ.

5. ANÁLISE DE SOLUÇÕES POSSÍVEIS

5.1. PESQUISA DE SOLUÇÕES E REFERÊNCIAS DE MERCADO

5.1.1. Para a contratação em tela, foram pesquisados processos similares anteriores, feitos pelo TJCE e por outros órgãos e entidades, assim como pesquisa de oferta de soluções do mercado, com objetivo de identificar as diversas possibilidades e a existência de novas metodologias, tecnologias ou inovações que melhor supririam as necessidades do tribunal.

5.1.2. A consulta feita ao Portal Nacional de Contratações Públicas – PCNP, com o objetivo de identificar padrões de contratação e modelos de fornecimento adotados por outros órgãos públicos, revelou os editais e contratos vigentes, conforme demonstrado na tabela abaixo:

Tabela 3 - Consulta ao PCNP com contratações similares

Tipo	Modalidade	ID	Órgão	Solução	Valor total estimado	Vigência (Meses)	Valor/Mês
Editais	Pregão	13937032000160-1-002387/2024	PRODEB	Appliance	R$ 1.422.489,60	24	R$ 59.270,40
Editais	Pregão	08761132000148-1-000054/2024	SEFAZ-PB	VM	R$ 650.000,00	60	R$ 10.833,33
Contratos	Pregão	83279448000113-2-000044/2025	TCE-SC	SaaS	R$ 858.000,00	36	R$ 23.833,33
Editais	Pregão	00394445000101-1-000079/2025	MEC	Appliance	R$ 4.032.760,38	60	R$ 67.212,67
Editais	Pregão	04381083000167-1-000030/2025	MP-RO	Appliance	R$ 1.420.000,00	36	R$ 39.444,44
Contratos	Dispensa	00508903000188-2-002456/2024	TRF/1º	SaaS	R$ 839.242,08	24	R$ 34.968,42
Contratos	Dispensa	00508903000188-2-001352/2024	TRF/1º	Appliance	R$ 2.614.200,00	60	R$ 43.570,00
Contratos	Pregão	60265576000102-2-000006/2024	TJM-SP	SaaS	R$ 899.781,72	36	R$ 24.993,94
Contratos	Pregão	04801221000110-2-000026/2024	TCE-RO	SaaS	R$ 794.000,00	36	R$ 22.055,56
Contratos	Pregão	00488478000102-2-000171/2023	STJ	Appliance	R$ 2.849.077,00	60	R$ 47.484,62
Contratos	Pregão	83845701000159-2-000001/2023	TJ-SC	Appliance	R$ 3.890.000,00	60	R$ 64.833,33
Contratos	Dispensa	40176679000199-2-000005/2025	BIBLIOTECA	SaaS	R$ 7.473,00	12	R$ 622,75
Contratos	Pregão	10914290000132-2-000001/2025	CISAN-RO	SaaS	R$ 171.000,00	12	R$ 14.250,00
Contratos	Dispensa	05475103000121-2-000029/2024	SEGOV-MG	SaaS	R$ 268.206,00	12	R$ 22.350,50
Contratos	Dispensa	16745465000101-2-000041/2024	AGE-MG	SaaS	R$ 2.088,00	12	R$ 174,00
Contratos	Pregão	00394411000109-2-000152/2024	PRESIDÊNCIA	Appliance	R$ 3.884.000,00	60	R$ 64.733,33
Contratos	Dispensa	19377514000199-2-000014/2024	SEDE-MG	SaaS	R$ 11.232,00	12	R$ 936,00
Contratos	Dispensa	00488478000102-2-000123/2023	STJ	SaaS	R$ 1.130.472,24	24	R$ 47.103,01
Contratos	Dispensa	05461142000170-2-000078/2024	SEPLAG-MG	VM	R$ 4.193.352,60	60	R$ 69.889,21
Contratos	Pregão	05532085000172-2-000046/2024	TJ-MS	VM	R$ 1.350.000,00	36	R$ 37.500,00
Contratos	Dispensa	09263130000191-2-000009/2024	SUDENE	SaaS	R$ 367.358,40	60	R$ 6.122,64
Contratos	Dispensa	37115375000107-2-000001/2024	MEIO AMBIENTE	SaaS	R$ 1.425.229,20	60	R$ 23.753,82
Contratos	Dispensa	00394429000100-2-000963/2024	AERONAUTICA	SaaS	R$ 725.724,72	36	R$ 20.159,02
Contratos	Dispensa	08829974000194-2-000199/2024	ICMBIO	SaaS	R$ 1.057.034,40	12	R$ 88.086,20
Contratos	Dispensa	01468760000190-2-000025/2024	MP-SP	SaaS	R$ 419.621,04	12	R$ 34.968,42
Contratos	Pregão	13100722000160-2-000004/2025	TJ-BA	Appliance	R$ 3.476.759,46	60	R$ 57.945,99
Contratos	Dispensa	10377679000196-2-000215/202	JABOATÃO/PE	SaaS	R$ 105.703,44	12	R$ 8.808,62
Editais	Pregão	28127603014802-1-000003/2025	BANESTES	SaaS	R$ 1.650.230,00	60	R$ 27.503,83
Editais	Pregão	00394411000109-1-000226/2024	IMPRENSA	SaaS	R$ 901.111,00	60	R$ 15.018,52
Contratos	Dispensa	02292266000180-2-000101/2024	TJ-GO	SaaS	R$ 2.538.395,28	36	R$ 70.510,98

5.1.3. Foram identificados 30 registros de contratações referentes ao objeto WAF, distribuídos conforme o tipo de solução: **19 contratações na modalidade SaaS (63%), 8 na modalidade Appliance (27%) e 3 na modalidade baseada em Máquina Virtual (10%)**. Esses dados reforçam a predominância da solução SaaS entre os órgãos públicos, indicando uma tendência de mercado.

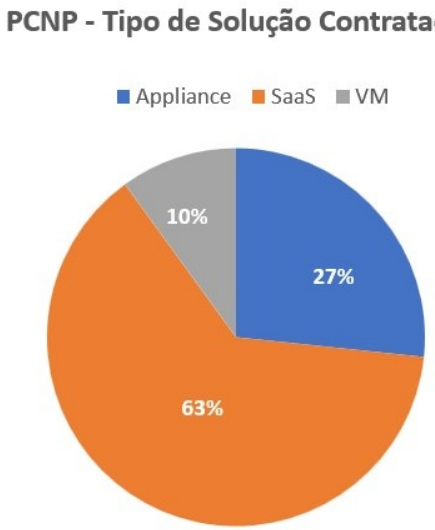

Gráfico 1 - Tipos de Soluções Contradas no PCNP

5.1.4. Complementando o levantamento anterior, foi realizado um inventário dos registros DNS do tipo "Start of Authority" (SOA) dos tribunais. Esse inventário permitiu mapear o tipo e infraestrutura atual — própria ou em nuvem — dos ambientes de serviço de nomes dos TJs, TRTs e tribunais superiores, fornecendo uma visão geral da maturidade na adoção de soluções em nuvem e subsidiando a escolha da solução WAF mais adequada às necessidades do TJCE.

Tabela 4 – Registro SOA no DNS dos Tribunais

DNS SOA - TRIBUNAIS			
ÓRGÃO	**DOMAIN**	**MNAME**	**INFRAESTRUTURA**
TJ	tjac.jus.br	nsnbs.tjac.jus.br	Tribunal
TJ	tjal.jus.br	alfa.tjal.jus.br	Tribunal
TJ	tjap.jus.br	dns.cloudflare.com	Nuvem
TJ	tjam.jus.br	ns1.tjam.jus.br	Tribunal
TJ	tjba.jus.br	ns3.tjba.jus.br	Tribunal
TJ	tjce.jus.br	ns1.tjce.jus.br	Tribunal
TJ	tjdft.jus.br	ns1-35.azure-dns.com	Nuvem
TJ	tjes.jus.br	ns-1117.awsdns-11.org	Nuvem
TJ	tjgo.jus.br	dns.cloudflare.com	Nuvem
TJ	tjma.jus.br	ns1.tjma.jus.br	Tribunal
TJ	tjmt.jus.br	ns-01.tjmt.jus.br	Tribunal
TJ	tjms.jus.br	ns1.tjms.jus.br	Tribunal
TJ	tjmg.jus.br	ns4.tjmg.jus.br	Tribunal
TJ	tjpa.jus.br	ns.tjpa.jus.br	Tribunal
TJ	tjpb.jus.br	coqueirinho.tjpb.jus.br	Tribunal
TJ	tjpr.jus.br	ns1.tjpr.jus.br	Tribunal
TJ	tjpe.jus.br	ns-381.awsdns-47.com	Nuvem
TJ	tjpi.jus.br	ns1.tjpi.jus.br	Tribunal
TJ	tjrj.jus.br	ms1.tjrj.jus.br	Tribunal
TJ	tjrn.jus.br	a1-38.akam.net	Nuvem
TJ	tjrs.jus.br	ns.tjrs.jus.br	Tribunal
TJ	tjro.jus.br	srvns1.tjro.jus.br	Tribunal
TJ	tjrr.jus.br	ns1.tjrr.jus.br	Tribunal
TJ	tjsc.jus.br	ns.tjsc.jus.br	Tribunal
TJ	tjsp.jus.br	ns-2018.awsdns-60.co.uk	Nuvem
TJ	tjse.jus.br	ns01.tjse.jus.br	Tribunal
TJ	tjto.jus.br	ns.tjto.jus.br	Tribunal
TRT	trt14.jus.br	ns-1918.awsdns-47.co.uk	Nuvem
TRT	trt19.jus.br	ns-348.awsdns-43.com	Nuvem
TRT	trt11.jus.br	ns-1731.awsdns-24.co.uk	Nuvem
TRT	trt5.jus.br	ns-1876.awsdns-42.co.uk	Nuvem
TRT	trt7.jus.br	ns-254.awsdns-31.com	Nuvem
TRT	trt10.jus.br	ns-380.awsdns-47.com	Nuvem
TRT	trt17.jus.br	ns-1924.awsdns-48.co.uk	Nuvem
TRT	trt18.jus.br	ns-1525.awsdns-62.org	Nuvem
TRT	trt16.jus.br	dns01.trt16.jus.br	Tribunal
TRT	trt3.jus.br	ns-518.awsdns-00.net	Nuvem
TRT	trt24.jus.br	ns-425.awsdns-53.com	Nuvem
TRT	trt23.jus.br	ns-23.awsdns-02.com	Nuvem
TRT	trt8.jus.br	ns-558.awsdns-05.net	Nuvem
TRT	trt13.jus.br	ns-1703.awsdns-20.co.uk	Nuvem
TRT	trt6.jus.br	ns1.trt6.jus.br	Tribunal
TRT	trt22.jus.br	ns-1414.awsdns-48.org	Nuvem
TRT	trt9.jus.br	ns-319.awsdns-39.com	Nuvem
TRT	trt1.jus.br	ns-687.awsdns-21.net	Nuvem

TRT	trt21.jus.br	ns-560.awsdns-06.net	Nuvem
TRT	trt14.jus.br	ns-1918.awsdns-47.co.uk	Nuvem
TRT	trt8.jus.br	ns-558.awsdns-05.net	Nuvem
TRT	trt4.jus.br	ns-326.awsdns-40.com	Nuvem
TRT	trt12.jus.br	ns-827.awsdns-39.net	Nuvem
TRT	trt20.jus.br	ns-1070.awsdns-05.org	Nuvem
TRT	trt2.jus.br	ns-757.awsdns-30.net	Nuvem
TRT	trt18.jus.br	ns-1525.awsdns-62.org	Nuvem
Superior	stf.jus.br	ns-1363.awsdns-42.org	Nuvem
Superior	tst.jus.br	ns-1065.awsdns-05.org	Nuvem
Superior	stj.jus.br	dns.cloudflare.com	Nuvem
Superior	tse.jus.br	ns-1088.awsdns-08.org	Nuvem

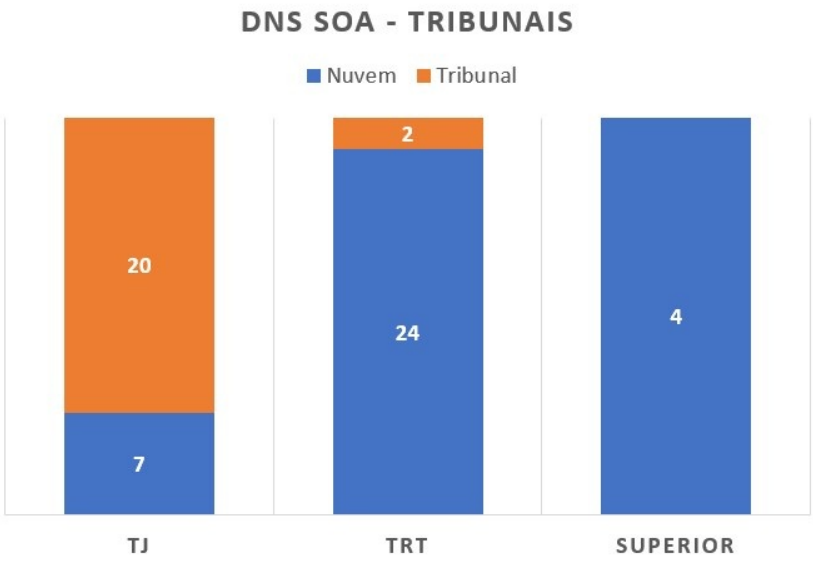

Gráfico 2 - DNS Authority Record dos Tribunais

5.1.5. No cenário levantado, observa-se que, entre os Tribunais de Justiça (TJs), 20 estão alocados em ambiente "Tribunal" e apenas 7 em "Nuvem", ao passo que, nos Tribunais Regionais do Trabalho (TRTs), 24 encontram-se em "Nuvem" e 2 em "Tribunal". Isso revela uma adoção significativamente maior de soluções em nuvem no âmbito dos TRTs, enquanto os TJs ainda mantêm predominância de infraestrutura própria.

5.1.6. Adicionalmente, essa migração foi viabilizada pela Ata de Registro de Preços nº 05/2022 do TRT da 4ª Região — instrumento que padronizou a contratação de serviços de proteção de borda de rede, CDN integrada a WAF e mitigação DDoS via SaaS por 36 meses. A ampla adesão a essa ata demonstra a maturidade das soluções de segurança em nuvem no mercado, refletindo não apenas ganhos em eficiência operacional, mas também a crescente convergência dos tribunais às soluções disponíveis em nuvem.

5.1.7. Esse movimento justifica-se pela necessidade de elevar a resiliência e a escalabilidade dos serviços e da camada de segurança. A computação em nuvem oferece distribuição geográfica inteligente, escalonamento sob demanda e integração nativa das CDNs com soluções de mitigação DDoS. Assim, adotar WAF na nuvem reduz pontos únicos de falha, assegura alta disponibilidade mesmo sob picos de tráfego malicioso e simplifica atualizações de regras de segurança — ganhos essenciais para órgãos que demandam 24×7 de proteção perimetral.

5.1.8. Nos quatro tribunais superiores (STF, TST, STJ e TSE), todos os servidores DNS autoritativos já rodam em "Cloud" (AWS ou Cloudflare). Esse cenário reforça a tendência de adoção plena da nuvem nessas instâncias, indicando sua confiabilidade e maturidade para serviços críticos de segurança e disponibilidade.

5.1.9. Essas informações subsidiaram a análise de aderência e viabilidade técnico-econômica da solução a ser contratada.

5.2. ANÁLISE COMPARATIVA DE SOLUÇÕES

Tabela 5 - Resumo da análise comparativa de soluções ADC e WAF

Requisito		(A) WAF SaaS	(B) GovShield	(C) Hardware	(D) Software Livre	(E) Netscaler
ADC	RT-01 ADC			X	X	X
	RT-04 Alta Disponibilidade	X	X	X	X	X
	RT-05 Treinamento	X	X	X		
	RT-06 Suporte	X	X	X		

Requisito		(A) WAF SaaS	(B) GovShield	(C) Hardware	(D) Software Livre	(E) Netscaler
	RT-02 WAF	X	X	X		X
	RT-03 Escalabilidade	X	X			
	RT-07 DNSSec	X	X	X		X

WAF	RT-08 Híbrido	X	X			
	RT-09 Latência	X	X	X		X
	RT-10 Anti-bot	X	X	X		X
	RT-11 Proteção de APIs	X	X	X		X
	RT-04 Alta Disponibilidade	X	X	X	X	X
	RT-05 Treinamento	X	X	X		
	RT-06 Suporte	X	X	X		

5.2.1. **Solução A** – WAF em nuvem como Serviço (**SaaS**)

5.2.1.1. **Contratação** do WAF em nuvem como serviço oferece proteção especializada para aplicações web por meio de infraestrutura distribuída, eliminando a necessidade de investimento em hardware local. O modelo sob demanda permite alocação dinâmica de recursos, garantindo atualizações automáticas de segurança, monitoramento contínuo e redundância geográfica. A solução opera na borda da rede (edge), normalmente integrada a serviços de CDN e mecanismos de mitigação distribuída de ataques DDoS, permitindo proteção escalável e baixa latência. Além disso, pode proteger aplicações hospedadas tanto em ambientes em nuvem quanto on-premises, facilitando a integração entre esses ambientes e operação única. A adoção do modelo SaaS também acompanha as tendências observadas nas pesquisas de mercado, que indicam preferência crescente por esse tipo de solução em contratações recentes no setor público.

5.2.2. **Solução B** – **GovShield** (SERPRO)

5.2.2.1. **Dispensa de licitação** com a plataforma GovShield, ofertada pelo Serpro e apoiada na infraestrutura da Cloudflare, disponibiliza proteção (WAF) e distribuição de aplicações (CDN) como serviço. Por ser prestada diretamente por um ente público de TI, sua contratação pode ocorrer por dispensa de licitação, agilizando o processo e reduzindo burocracia. Essa solução está alinhada às políticas de transformação digital do setor público e elimina a necessidade de investimentos em hardware próprio.

5.2.3. **Solução C** – **Aquisição** de solução disponível no mercado (appliance físico)

5.2.3.1. **Aquisição** de uma solução licenciada disponível no mercado, que pode ser fornecida na forma de appliance físico, integrando as funcionalidades de WAF e ADC em uma única plataforma. Embora tecnicamente viável para suportar o volume de tráfego atual e futuro, essa abordagem exige que todo o tráfego destinado a aplicações em nuvem seja roteado pela infraestrutura interna do TJCE. Esse modelo eleva o custo de investimento inicial.

5.3. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

5.3.1. **Solução D** – **Software Livre**

5.3.1.1. O ADC implantado em máquinas virtuais, utilizando software open source como HAProxy ou NGINX, oferece balanceamento de carga e terminação SSL/TLS. Essa solução é escalável, permitindo crescimento horizontal e vertical conforme a demanda, além de suportar alta disponibilidade com arquitetura ativa-standby e failover automático. Com a migração de aplicações críticas para a nuvem, a infraestrutura local fica menos sobrecarregada, possibilitando a substituição de equipamentos dedicados por soluções virtualizadas, reduzindo custos e mantendo o desempenho esperado.

5.3.1.2. Entretanto, constatou-se que a solução em análise não configura uma contratação típica, razão pela qual não se correlaciona, de forma direta, com os requisitos de treinamento (RT-05) e suporte (RT-06). Até o momento, não há nenhum retorno registrado sobre contratos ou editais relacionados à ferramenta HAProxy no PCNP (Portal de Compras do Governo). Como se trata de uma solução essencialmente baseada em software livre, o uso do HAProxy não depende de contratação formal via licitação ou edital. No entanto, essa característica também implica que sua implementação e manutenção exigem envolvimento técnico interno. A adoção do HAProxy requer que a equipe responsável tenha expertise em Linux, uma vez que grande parte da configuração, do tuning e da integração do balanceador de carga é manual e customizada, sem o suporte tradicional de contratos comerciais. Nesse cenário, torna-se essencial recorrer à comunidade ativa para troca de soluções e boas práticas.

Figura 2 - Resultado da pesquisa do termo "haproxy" no PCNP

5.3.1.3. Adicionalmente, foi realizada uma Prova de Conceito (POC) internamente, na qual se identificou grande dificuldade na migração das regras atualmente em vigor no NetScaler para o HAProxy, em especial devido ao número elevado de políticas, que ultrapassa 1.500 objetos. Esse volume torna a transposição complexa, sobretudo considerando que a solução em software livre depende primordialmente de suporte de comunidade.

Figura 3 - Resumo da configuração balanceamento de carga do Netscaler

5.3.1.4. Ressalta-se, ainda, que a solução exerce um papel central e crítico na infraestrutura, com configurações avançadas não apenas de balanceamento de carga, mas também de content switching e rewrite. Nesse contexto, a especificidade e complexidade das configurações aumenta significativamente o risco operacional, reforçando a inviabilidade de sua adoção.

5.3.1.5. Algumas observações sobre a Prova de Conceito (POC) realizada para Estudo para Substituição do Netscaler por Solução Open Source:

Em análise ao possível uso do HAProxy como substituto do NetScaler (Citrix ADC) no ambiente do TJCE, preparamos um comparativo técnico com foco nas funcionalidades que já são utilizadas atualmente. Listamos abaixo os principais recursos que o HAProxy, na versão open source, não oferece de forma nativa, mas que estão presentes no NetScaler e fazem diferença no contexto da nossa infraestrutura:

Conclusão: Embora o HAProxy possa atender demandas básicas de balanceamento L4/L7, ele não substitui integralmente o NetScaler em ambientes que exigem:

·Segurança perimetral robusta
·Alta disponibilidade com failover automatizado
·Integração com DNS e gestão de certificados
·Monitoramento centralizado e visibilidade operacional
·Facilidade de gerenciamento por interface gráfica

1. Falta de Interface Gráfica Nativa

O HAProxy não possui interface gráfica para configuração e monitoramento na versão open source. Toda a gestão é feita via arquivos de configuração em texto plano, sem painel web para políticas, métricas ou alertas.

2. Recursos de Segurança Avançados ausentes

O HAProxy não oferece WAF (Firewall de Aplicação Web) nativamente; só é possível via integrações complexas com ModSecurity.

Não há suporte a proteção contra DDoS, IP reputation, controle de bots ou análise comportamental de tráfego.

Tais funcionalidades são incorporadas diretamente no NetScaler e amplamente utilizadas para garantir segurança perimetral.

3. Ausência de suporte a DNSSEC

O HAProxy não oferece suporte à validação ou assinatura DNSSEC, o que pode comprometer a integridade e autenticidade de resoluções DNS em ambientes que demandam esse nível de segurança.

O NetScaler, por outro lado, suporta DNSSEC nativamente, inclusive para zonas autoritativas.

4. Alta Disponibilidade menos integrada

Embora o HAProxy suporte HA via ferramentas como Keepalived (VRRP), isso exige configuração externa e manutenção separada.

O NetScaler já oferece failover automático com sincronismo completo entre instâncias, reduzindo pontos de falha e esforço operacional.

5. TLS termination com gerenciamento limitado

O HAProxy permite TLS termination, mas não possui gerenciamento completo de certificados, SNI, ciphers e políticas TLS via GUI.

O NetScaler oferece interface para gestão completa de certificados, renovação automatizada e políticas granulares de segurança TLS.

6. Gerenciamento de certificados wildcard e integração com DNS

No NetScaler, certificados wildcard podem ser gerenciados centralmente e aplicados de forma automática a múltiplos serviços e domínios, com integração direta aos serviços DNS. Isso garante que, ao atualizar um certificado, ele seja automaticamente refletido nas zonas e entradas DNS configuradas.

Já no HAProxy, não há integração nativa com DNS nem automação da distribuição de certificados. A aplicação de certificados wildcard exige:

·Scripts personalizados para renovação e reload de configuração
·Ausência de propagação automática para outros serviços DNS ou instâncias

7. Monitoramento e visibilidade operacional limitados

O HAProxy oferece uma interface web básica para métricas e requer configuração adicional (com Prometheus, Grafana ou ferramentas similares) para visualizações mais completas.

Não há análise detalhada de tráfego, nem logging avançado de políticas ou sessões. O troubleshooting também é mais técnico e descentralizado.

O NetScaler, por sua vez, fornece monitoramento avançado e integrado, com:

·Dashboards gráficos em tempo real, exibindo tráfego, erros, latência, SSL e políticas aplicadas
·Logging e auditoria completos para sessões e regras
·Análise de tráfego em camadas L4 e L7, facilitando a detecção de anomalias, falhas ou degradação de serviços.

5.3.2. **Solução E** – Citrix **NetScaler** (atual)

5.3.2.1. Os appliances Citrix NetScaler em operação no TJCE apresentam CPU com picos de 100% de utilização e mostram sinais de saturação no processamento de pacotes e SSL offload. A continuidade deste modelo, sem upgrade de hardware, implicaria risco elevado de indisponibilidade, degradação de desempenho e impossibilidade de aplicar novas políticas de segurança sem comprometer o desempenho do equipamento.

5.3.2.2. A seguir, apresenta-se o gráfico de utilização de CPU dos appliances NetScaler durante o último mês, bem como o volume total de requisições processadas, demonstrando o esgotamento da capacidade atual. A eventual implementação do serviço de WAF nesse cenário torna-se um fator crítico, pois adicionaria carga adicional ao processamento, acentuando ainda mais o risco de saturação e comprometendo a estabilidade do ambiente.

Figura 4 - Utilização da CPU nos appliances Citrix NetScaler do TJCE

5.3.2.3. Portanto, diante da saturação observada e da incapacidade da solução atual de escalar conforme a demanda, fica evidente que manter o modelo vigente não atende ao RT-03 de escalabilidade.

5.3.2.4. Foi realizada uma busca no Portal Nacional de Contratações Públicas (PNCP) para verificar a existência de editais, avisos de contratação, atas de registro de preços e contratos vigentes ou não vigentes relacionados à solução Citrix NetScaler. O resultado da pesquisa indicou ausência de registros para o termo “netscaler” nas categorias consultadas, com exceção do contrato nº CT-024/2023 de 2023, firmado pelo próprio TJCE.

5.3.2.5. Essa ausência de referências é relevante para o processo de contratação. Primeiramente, a inexistência de contratações recentes ou em andamento para a solução Citrix NetScaler em outros órgãos públicos pode indicar que o equipamento não está sendo adotado amplamente no setor público atualmente. Tal cenário pode refletir um possível desuso, obsolescência tecnológica ou mesmo uma tendência de mercado que aponta para a preferência por soluções alternativas ou de outros fabricantes.

5.3.2.6. Adicionalmente, foram realizadas tentativas de contato, durante o mês de maio de 2025, com diversas empresas parceiras da Citrix para obtenção de propostas comerciais. O retorno foi parcial: algumas empresas, como LGTI, RGK4IT, Inbtec e Quales, responderam, porém não encaminharam propostas; outras, como Addvalue, Niva, Alsar, Emx e Mahvla, não retornaram; enquanto a Vectra informou que não atende à Citrix. Ressalta-se que, até a finalização da presente versão do ETP, as empresas que não haviam respondido permanecem sem retorno.

5.3.2.7. A baixa adesão e o interesse limitado de fornecedores qualificados indicam possíveis dificuldades para viabilizar a contratação da solução Citrix NetScaler. Esse cenário pode estar relacionado, principalmente, ao fim da vida útil do equipamento previsto para 2028, o que reduz o horizonte de suporte e desestimula a formalização de contratos de curta duração.

5.3.2.8. Além disso, essa dependência pode implicar em risco elevado de aprisionamento tecnológico (vendor lock-in), restringindo a flexibilidade e autonomia do TJCE para futuras atualizações ou mudanças tecnológicas. A ausência de múltiplas propostas competitivas e a escassez de editais semelhantes em outros órgãos públicos reforçam o risco de insucesso no processo licitatório, podendo levar ao fracasso do certame ou a condições contratuais desfavoráveis, comprometendo a segurança e continuidade dos serviços.

5.3.2.9. Portanto, a combinação da ausência de registros no PNCP, a reduzida resposta do mercado fornecedor e a baixa utilização da solução Citrix NetScaler em outros órgãos públicos evidenciam a inviabilidade da contratação dessa tecnologia neste momento, que não atende ao RT-06 de Suporte.

6. PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÃO ANUAL

6.1. A contratação ora pretendida está em consonância com os objetivos estratégicos deste TJCE (conforme Planejamento Estratégico 2021–2030), visto que prevê o fortalecimento da infraestrutura tecnológica por meio da adoção de soluções inovadoras, escaláveis e seguras, o que é imprescindível para o funcionamento do TJCE no desempenho de suas atividades institucionais, alinhando-se diretamente aos objetivos de transformação digital, segurança da informação e sustentabilidade orçamentária.

6.2. O objeto da contratação está previsto no Plano de Contratações Anual 2026, especificamente no Código da Contratação RDP-SETIN-2026-26.

7. REQUISITOS DA CONTRATAÇÃO

7.1. A empresa deve possuir estrutura e experiência em fornecimentos compatíveis com objeto demandado;

7.2. Nos casos de fornecimentos, ou parte deles, controlados ou de exercício mediante autorização prévia, caberá à empresa a regularização e obtenção de respectiva(s) licença(s) ou registro(s);

7.3. No caso de produtos de mercado restrito, a empresa deverá certificar-se, ainda antes de eventual participação em licitação ou contratação, de que possui fabricantes ou fornecedores aptos ao tipo de objeto requerido nesta demanda.

7.4. Comprovar, como condição prévia à assinatura do contrato e para a manutenção contratual, o atendimento das seguintes condições:

7.4.1. Não possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pela Portaria Interministerial MTPS/MMIRDH Nº 4 DE 11/05/2016;

7.4.2. Não ter sido condenada, a EMPRESA ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta a previsão aos artigos 1° e 170 da Constituição Federal de 1988; do artigo 149 do Código Penal Brasileiro; do Decreto n° 5.017, de 12 de março de 2004 (promulga o Protocolo de Palermo) e das Convenções da OIT nos 29 e 105;

7.5. A solução a ser contratada deverá estar vinculada a contrato de suporte técnico ativo, com cobertura 24x7x365, compatível com as necessidades de operação contínua da instituição. O suporte deverá incluir atendimento técnico especializado, correção de falhas, atualização de versões e demais serviços necessários à plena disponibilidade do sistema, mantendo-se ativo durante toda a vigência contratual.

7.6. A instalação física dos equipamentos, bem como a configuração inicial, integração com o ambiente tecnológico existente e demais procedimentos necessários para a plena entrada em operação da solução, devem seguiras boas práticas de implantação e garantir seu correto funcionamento no ambiente da instituição.

7.7. O fornecimento de treinamento técnico remoto para a equipe interna, com o objetivo de garantir a correta operação, configuração e manutenção da nova solução. O formato remoto visa assegurar economicidade e viabilidade logística, considerando a necessidade de rápida capacitação do corpo técnico.

8. ESTIMATIVAS DE QUANTIDADE

8.1. Durante a análise comparativa (seção 5.2) constatou-se que nenhuma das opções atendem integralmente todos os requisitos levantados. O principal motivo é o caráter híbrido do ambiente — recursos distribuídos entre nuvem e on-premises — no qual aplicações expostas à internet e aplicações internas acessadas por rede MPLS possuem requisitos técnicos distintos de processamento, latência e segurança, o que gera conflitos práticos quando se tenta resolver tudo com uma única solução integrada ou monolítica (all-in-one).

8.2. Segundo o Cloud End-User Behavior Survey da Gartner (ID G00811980, 20 maio 2024), 81% das empresas operam em múltiplos ambientes de nuvem pública e 55% também mantêm nuvens privadas. Essas mesmas organizações apontam a gestão de riscos de cibersegurança e a complexidade técnica como os dois principais desafios decorrentes do uso de múltiplos provedores, o que reforça que a adoção de modelos híbridos e multicloud é massiva e impõe barreiras relevantes de integração e segurança. Como resultado, muitas organizações optam por uma abordagem do melhor software por domínio (best-of-breed), adotando soluções especializadas para cada área crítica, reconhecidas como líder em sua categoria ou nicho específico, justamente para garantir que cada requisito técnico seja atendido adequadamente.

8.3. Diante disso, a alternativa mais prática e técnica é adotar soluções especializadas — por exemplo, um WAF dedicado e um ADC dedicado — porque cada solução especializada consegue cumprir seu conjunto de requisitos sem comprometer as garantias exigidas pela operação. Em função do exposto, apresenta as estimativas organizadas em Lote 1 (ADC) e Lote 2 (WAF), permitindo que cada item seja dimensionado, testado e contratado segundo critérios técnicos e contratuais próprios, sem dependências que aumentem risco ou complexidade desnecessária.

8.4. Na observância do volume da necessidade e seu detalhamento, foram considerados para o Lote1 - ADC:

8.4.1. As especificações técnicas do equipamento atualmente em uso, modelo 8920, foram utilizadas como referência de capacidade mínima, considerando suas principais características operacionais, como memória de 32 GB, 4 interfaces de acesso, throughput de tráfego de 20 Gbps e capacidade de processamento SSL (SSL bulk) de 20 Gbps. Esses parâmetros refletem não apenas o volume de tráfego suportado, mas também a necessidade de elevado processamento criptográfico para terminação de conexões SSL/TLS, função essencial para aplicações seguras hospedadas no datacenter institucional, servindo de base para a estimativa dos quantitativos da contratação.

8.4.2. Adicionalmente, considerou-se que o novo core de rede mantém velocidades de acesso de 10 e 25 Gbps, razão pela qual foram previstas interfaces de 40 Gbps na solução, com o objetivo de evitar congestionamentos e ocorrência de output drops nas interfaces de agregação, tendo em vista a característica da topologia adotada, na qual o padrão de tráfego é predominantemente do tipo many-to-one.

8.4.3. Resumo das configurações do appliance evidenciou a presença de 620 Load Balancing Virtual Servers, 543 Servers, além de 192 Content Switching Virtual Servers, 866 Content Switching Policies:

Figura 5 - Resumo da configuração balanceamento de carga do Netscaler

8.4.4. Além disso, a solução a ser contratada deverá estar vinculada a contrato de suporte técnico ativo, com cobertura 24x7x365, compatível com as necessidades de operação contínua da instituição. O suporte deverá incluir atendimento técnico especializado, correção de falhas, atualização de versões e demais serviços necessários à plena disponibilidade do sistema, mantendo-se ativo durante toda a vigência contratual.

8.4.5.A contratada deverá realizar a instalação física dos equipamentos, bem como a configuração inicial, integração com o ambiente tecnológico existente e demais procedimentos necessários para a plena entrada em operação da solução, observando as boas práticas de implantação e garantindo seu correto funcionamento no ambiente da instituição.

8.4.6.Deverá ser previsto o fornecimento de treinamento técnico remoto para a equipe interna, com o objetivo de garantir a correta operação, configuração e manutenção da nova solução. O formato remoto visa assegurar economicidade e viabilidade logística, considerando a necessidade de rápida capacitação do corpo técnico.

8.4.7. Com o objetivo de consolidar as informações levantadas e facilitar o entendimento dos requisitos técnicos e quantitativos da demanda, será incluída uma tabela com os principais itens relacionados à contratação da nova solução do lote 1 - ADC:

Tabela 6 - Estimativas De Quantidade para o Lote 1

Lote 1			
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QUANTIDADE**
1	Solução balanceador de carga/controlador de entrega de aplicações (ADC)	UND	02
2	Suporte 24x7x365 à solução contratada durante a vigência contratual	Mês	57
3	Treinamento remoto da solução para até 08 participantes	Alunos	08
4	Instalação	UND	02

8.5. Na observância do volume da necessidade e seu detalhamento, foram considerados para o Lote2 - WAF:

8.5.1. A tabela a seguir apresenta o volume de dados registrado no firewall de borda ao longo dos últimos 90 dias, considerando apenas aplicações SSL/Web Browsing oriundas da zona de Internet. Observa-se a média apurada no período foi de aproximadamente 1,67 TB/dia, resultando em uma projeção mensal da ordem de 50 TB/mês. Esse valor é utilizado como base para dimensionamento da franquia mensal do serviço, refletindo o comportamento recorrente do ambiente, devendo ser considerado como referência de consumo base, sendo as variações e picos de tráfego absorvidos por meio de franquia adicional contratual.

Tabela 7 - Throughput de dados no firewall de borda nos últimos 90 dias.

Dia	**TB**
12/01/2006	1,83
13/01/2006	1,86
14/01/2006	1,86
15/01/2006	1,77
16/01/2006	1,51
17/01/2006	0,69
18/01/2006	0,69
19/01/2006	1,48
20/01/2006	1,97
21/01/2006	2,27
22/01/2006	2,13
23/01/2006	1,82
24/01/2006	0,86
25/01/2006	0,68
26/01/2006	1,74
27/01/2006	2,18
28/01/2006	2,06
29/01/2006	2,02
30/01/2006	2,00
31/01/2006	1,48
01/02/2006	1,68
02/02/2006	2,02
03/02/2006	2,23
04/02/2006	2,20
05/02/2006	2,09

Dia	TB
06/02/2006	1,99
07/02/2006	0,90
08/02/2006	0,81
09/02/2006	2,00
10/02/2006	2,35
11/02/2006	2,39
12/02/2006	2,33
13/02/2006	2,08
14/02/2006	0,97
15/02/2006	0,73
16/02/2006	0,86
17/02/2006	0,96
18/02/2006	1,58
19/02/2006	2,23
20/02/2006	2,11
21/02/2006	0,98
22/02/2006	0,88
23/02/2006	1,98
24/02/2006	0,72
25/02/2006	2,13
26/02/2006	1,98
27/02/2006	2,07
28/02/2006	0,93
01/03/2006	0,86
02/03/2006	2,03
03/03/2006	0,92
04/03/2006	2,36
05/03/2006	2,27
06/03/2006	2,00
07/03/2006	0,98
08/03/2006	0,92
09/03/2006	2,16
10/03/2006	1,06
11/03/2006	2,43
12/03/2006	2,40
13/03/2006	2,14
14/03/2006	1,13
15/03/2006	1,04
16/03/2006	2,28
17/03/2006	1,61
18/03/2006	2,32
19/03/2006	1,65
Méda	**1,67**

8.5.2. A figura abaixo apresenta o consumo de banda da interface de rede conectada à zona DMZ. Observa-se que o tráfego atinge picos de utilização de aproximadamente 500 Mbps, refletindo a intensidade das comunicações entre os serviços publicados nessa zona pública e as demais camadas da rede institucional. O comportamento do gráfico demonstra variações compatíveis com o perfil de uso dos sistemas críticos hospedados no ambiente, indicando a necessidade de manutenção de capacidade adequada de throughput equivalente para evitar gargalos e assegurar a continuidade das operações.

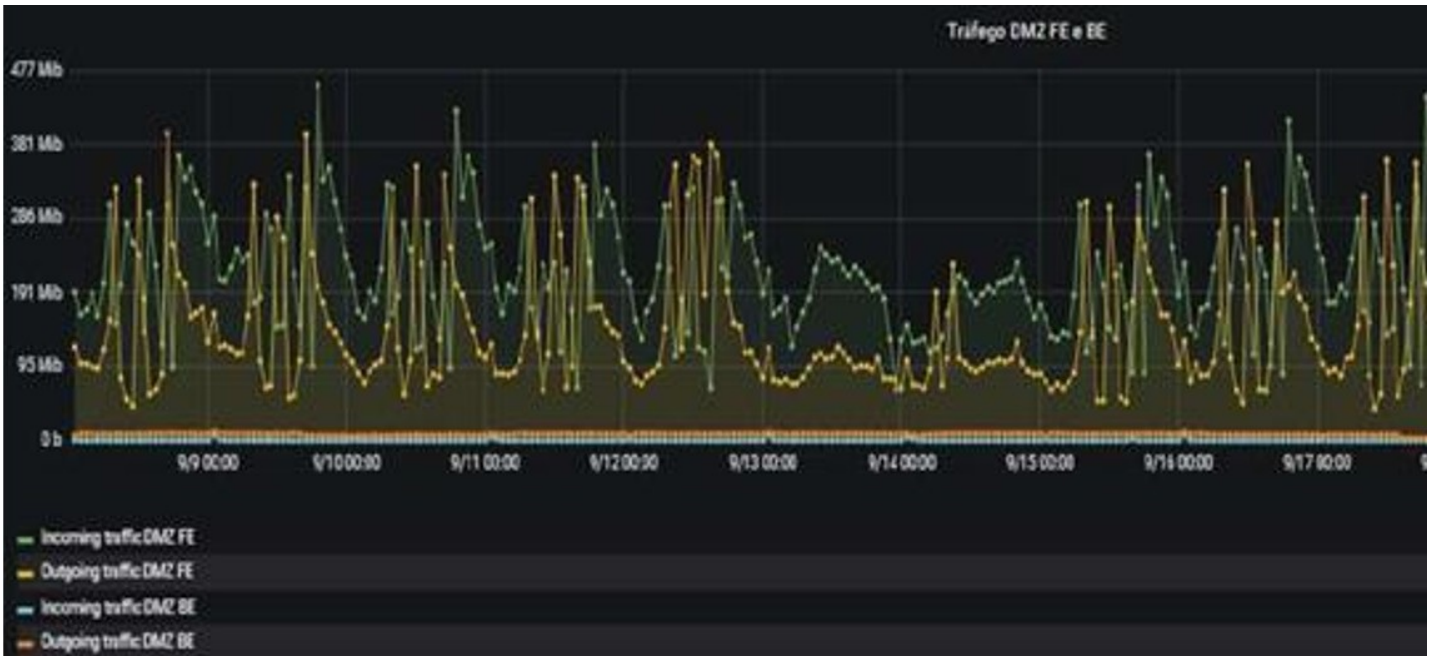

Figura 7 - Banda consumida nos últimos 15 dias, com picos até 500 Mbps.

8.5.3. Considerando a oscilação natural do tráfego em períodos de pico de acesso e a imprevisibilidade do volume de requisições em aplicações críticas expostas à internet, justifica-se a contratação de franquia adicional de tráfego limpo, a ser consumida e contratada sob demanda durante a vigência contratual.

8.5.3.1. Do ponto de vista técnico, o dimensionamento dessa franquia adicional apresenta limitações objetivas, uma vez que não há histórico consolidado superior a 12 (doze) meses específico para consumo em franquias de dados do tráfego de interesse da solução WAF. Ainda que existam gráficos de utilização em Kbps referentes aos links de internet, esses registros abrangem todo o tráfego de rede, incluindo comunicações internas e não apenas o tráfego externo direcionado às aplicações web (HTTP/HTTPS) — que é o foco de atuação do WAF. Dessa forma, a estimativa da franquia base foi obtida a partir de coletas recentes e mais representativas do comportamento atual, reconhecendo-se a limitação técnica de projeção mais precisa.

8.5.3.2. Sob o aspecto jurídico e administrativo, a previsão de franquia adicional sob demanda visa assegurar a continuidade do serviço essencial, evitando a indisponibilidade decorrente do esgotamento da franquia base e permitindo adequação dinâmica às necessidades reais de consumo durante a execução contratual. Trata-se de medida proporcional e vantajosa à Administração, que não encarece o objeto, pois o consumo adicional ocorrerá apenas quando comprovadamente necessário, mediante controle e comprovação de uso efetivo, em consonância com os princípios da eficiência, economicidade e continuidade do serviço público.

8.5.3.3. Complementarmente ao aspecto técnico exposto no item anterior, a previsão contratual de franquia adicional também se justifica sob o ponto de vista econômico e gerencial. A contratação sob demanda previamente estabelecida no instrumento contratual possibilita custos unitários previsíveis e inferiores aos praticados em contratações emergenciais, evitando reajustes intempestivos e reduzindo riscos de interrupção do serviço, os quais poderiam acarretar prejuízos operacionais e financeiros de maior impacto à Administração.

8.5.3.4. A metodologia de estimativa adotada considerou o consumo histórico médio mensal de aproximadamente 50 TB, valor obtido a partir de coletas recentes dos períodos de maior atividade. Por prudência técnica e em observância a continuidade do serviço, prevê-se a possibilidade de contratação adicional, assegurando elasticidade e escalabilidade à solução sem gerar aumento desproporcional de custos.

8.5.3.5. Tal percentual demonstra razoabilidade, pois não representa acréscimo excessivo sobre a franquia base, mas permite absorver variações sazonais e crescimento gradual do tráfego, compatível com o modelo elástico de serviços em nuvem, cujo consumo é ajustado conforme a demanda real. Na prática, a solução poderá crescer até 1,5 vezes o volume base — um acréscimo de 50% de capacidade — suficiente para absorver picos de tráfego, sazonalidades e expansões graduais durante a vigência do contrato. Essa margem de expansão controlada mitiga riscos de indisponibilidade e assegura continuidade operacional.

8.5.4. Resumo das configurações do appliance utilizado com DNSSEC evidenciou a presença de 255 FQDNs, todos vinculados à mesma zona DNS institucional. Dessa forma, a contratação de proteção de DNS para 1 (uma) zona mostra-se suficiente para abranger os registros atualmente utilizados, garantindo a proteção do domínio principal e de seus respectivos subdomínios, bem como suportando a criação de novos registros dentro da mesma zona:

Figura 8 - Resumo da configuração DNSSEC do Netscaler

8.5.5. Com o objetivo de consolidar as informações levantadas e facilitar o entendimento dos requisitos técnicos e quantitativos da demanda, será incluída uma tabela com os principais itens relacionados à contratação da nova solução do lote 2 - WAF:

Tabela 7 - Estimativas De Quantidade para o Lote 2

		Lote 2
ITEM	**DESCRIÇÃO**	**UNIDADE**

1	Web Application Firewall (WAF) em modelo Software como Serviço (SaaS), com franquia mensal de 50 TB de tráfego inspecionado.	Mês
2	Franquia adicional correspondente a até 50% da franquia base, aplicável ao volume total de tráfego (TB), disponível para consumo sob demanda durante a vigência contratual.	TB
3	Proteção DNS para 1 Zona	Mês

9. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

9.1. O Cálculo dos Custos Totais de Propriedade para o Lote 1 não foi elaborado com base em análise comparativa, uma vez que foi identificada predominância de soluções baseadas em appliance físico para ADC, em razão da maior capacidade de throughput e processamento de tráfego, característica necessária para suportar volumes elevados de requisições com baixa latência.. Ainda assim, foi realizado levantamento de mercado com o objetivo de subsidiar a análise econômica da solução e permitir a estimativa preliminar do custo da demanda, conforme evidenciado no mapa comparativo de preços, no qual o valor estimado do Lote 1 corresponde a **R$ 3.179.746,28**.

9.2. O Cálculo dos Custos Totais de Propriedade para o Lote 2:

9.2.1. **Solução A** – WAF em nuvem como Serviço (**SaaS**)

9.2.1.1. Custo estimado mensal de **R$ 3.624.951,24.**

9.2.1.2. Fonte: AQSETIN2025003 – Mapa Comparativo de Preços (média sanitizada)

9.2.2. **Solução B** – **GovShield**

9.2.2.1. Custo estimado mensal de **R$ 153.443,62.**

9.2.2.2. Composição: R$ 20.159,02/mês (franquia 5 TB) + 45 TB (franquia adicional) × R$ 2.961,88/mês = R$ 153.443,62/mês.

9.2.2.3. Fonte: Loja SERPRO (vide Figura 9 – Modalidade Ouro do GovShield)

Figura 9 - Loja SERPRO, Modalidade Ouro do GovShield. fonte: https://loja.serpro.gov.br/govshield

9.3. Mapa Comparativo dos Cálculos Totais de Propriedade (TCO)

9.3.1. A seguir, apresenta-se o Custo Médio das soluções analisadas. Comparando alternativas equivalentes e substituíveis — a análise foi segmentada por Lote:

Tabela 8 - Quadro-Resumo - Custo Médio da Soluções

Lote	Alternativa	Custo Total Estimado	Premissas	Fonte
Lote 1 – ADC	**Solução C – Appliance (Aquisição de Hardware)**	**R$ 3.179.746,28**	Média sanitizada do Mapa Comparativo, valor de R$ 3.179.746,29	Mapa Comparativo de Preços
Lote 2 – WAF	**Solução A – WAF em nuvem (SaaS)**	**R$ 100.693,09/Mês**	Média sanitizada do Mapa Comparativo, valor total do lote 2 de R$ 3.624.951,24 ÷ 36 meses	Mapa Comparativo de Preços
Lote 2 – WAF	**Solução B – GovShield (SERPRO)**	**R$ 153.443,62/Mês**	50 TB/mês: 5 TB (R$ 20.159,02) + 45 TB (franquia adicional) × R$ 2.961,88 = R$ 153.443,62	Loja SERPRO

9.3.2. Considerando as diversas formas para atender à necessidade descrita neste documento, foram adotados os valores aproximados acima para o fornecimento das soluções, obtidos no documento AQSETIN2025003 – Mapa Comparativo de Preços (médias sanitizadas) e na consulta direta à Loja SERPRO, que indicam como razoável a estimativa, pelos seguintes motivos:

9.3.2.1. A pesquisa realizada no Portal Nacional de Contratações Públicas (PNCP) identificou 30 contratações relacionadas ao objeto, número representativo para a embasar a pesquisa de preço, com base em contratações similares efetuadas por outros órgãos públicos.

9.3.2.2. Foi realizada consulta direta ao site da Loja SERPRO para levantamento de preços da solução GovShield (Solução B), obtendo-se valores atualizados praticados no mercado público, com base em oferta no canal oficial da fornecedora.

9.3.2.3. Todos os valores foram convertidos para custo médio mensal considerando as respectivas vigências

9.3.2.4. No Mapa Comparativo (AQSETIN2025003), utilizou-se média sanitizada para mitigar distorções de preços extremos e melhorar a representatividade da amostra

10. SOLUÇÃO ESCOLHIDA

10.1. Após as análises técnicas e econômico-financeiras realizadas, definiu-se como solução mais adequada a contratação de uma solução de mercado para balanceamento de carga e proteção de aplicações web. A solução é composta por duas camadas tecnológicas complementares: um Controlador de Entrega de Aplicações (Application Delivery Controller – ADC), responsável pelas funções de balanceamento de carga, otimização de tráfego, alta disponibilidade e terminação SSL/TLS, e um Web Application Firewall (WAF), destinado à proteção das aplicações contra ameaças na camada de aplicação. A adoção dessa arquitetura em camadas permite atender, de

forma integrada, aos requisitos de desempenho, disponibilidade e segurança das aplicações institucionais.

10.2. Embora componham uma solução funcionalmente integrada, as camadas tecnológicas apresentam características técnicas, modelos de fornecimento e mercados fornecedores distintos. Em razão disso, e com o objetivo de ampliar a competitividade do certame e possibilitar a participação de fornecedores especializados em cada tecnologia, a contratação será estruturada em dois lotes:

10.2.1. Lote 1 – Controlador de Entrega de Aplicações (ADC), por meio de aquisição de solução disponível no mercado, em appliance físico;

10.2.2. Lote 2 – Web Application Firewall (WAF), ofertado como serviço em nuvem no modelo SaaS.

10.3.A divisão em lotes constitui medida de organização da contratação e não implica fracionamento do objeto, uma vez que este permanece uno em sua finalidade. A medida visa ampliar a competitividade, permitir a participação de fornecedores especializados e assegurar maior eficiência na implementação, operação da solução e otimizar a execução contratual.

10.4.A segmentação por camadas promove especialização funcional e atende diretamente aos requisitos: o WAF concentra-se na proteção das aplicações web (RT-02 WAF), enquanto o ADC foca na entrega e otimização do tráfego (RT-01 ADC). Essa separação possibilita evolução tecnológica e manutenção independentes, reduz o risco de impactos sistêmicos em atualizações, otimiza custos operacionais e aumenta a resiliência, alinhando-se às necessidades do TJCE e aos requisitos funcionais e técnicos previamente estabelecidos.

10.5.O modelo SaaS consiste na contratação de serviço em nuvem fornecido por provedor especializado, com cobrança recorrente, escalabilidade sob demanda (RT-03 Escalabilidade) e atualização contínua do serviço. Quando mediado por integrador, este responde pela gestão técnica e contratual. O processo compreende análise de necessidades, configuração, migração assistida, homologação e entrada em produção, com monitoramento permanente de suporte 24x7x365 (RT-06 Suporte).

10.6.A solução de Web Application Firewall (WAF) como serviço oferece proteção abrangente contra ameaças da OWASP Top 10, ataques DDoS, proteção de APIs (RT-11 Proteção de APIs) e mitigação de robôs automatizados (RT-10 Anti-Bot), com ativação ágil por alteração de DNS e sem exigência de infraestrutura física adicional. A presença de CDN contribui para baixa latência (RT-09) e alta disponibilidade (RT-04). O serviço inclui suporte, atualizações contínuas e portal de gestão, garantindo segurança, escalabilidade, conformidade com normas vigentes, compondo uma arquitetura moderna, modular e aderente ao cenário híbrido do TJCE (RT-08 Híbrido).

10.7.A aquisição de hardware dedicado para a função de ADC em ambiente on-premises permanece necessária para suportar o tráfego direcionado às aplicações hospedadas no datacenter local, especialmente aquelas acessadas por meio da rede MPLS corporativa. Esse tráfego interno não é encaminhado à internet pública e, portanto, não pode ser processado por soluções de segurança baseadas exclusivamente em nuvem sem introduzir latência adicional e dependência de conectividade externa.

10.8. Além disso, a terminação de conexões criptografadas (SSL/TLS) exige elevado poder de processamento, uma vez que envolve operações criptográficas intensivas. O uso de appliances dedicados permite a utilização de aceleração por hardware para processamento criptográfico e offload de SSL, garantindo maior throughput, menor latência e melhor desempenho no atendimento simultâneo de múltiplas conexões seguras.

10.9.A arquitetura fracamente acoplada — cada componente operando de forma modular e independente — favorece governança por SLAs, planejamento de capacidade, janelas de manutenção menores e estratégia de evolução tecnológica sem impacto cruzado entre camadas, em consonância com boas práticas de segurança em profundidade e continuidade de serviços.

10.10. Diante das análises e necessidades apresentadas, a escolha pela contratação do WAF como SaaS, se justifica pela robustez e pela segurança avançada que o serviço oferece, atendendo às exigências do Tribunal de Justiça do Estado do Ceará em termos de proteção e monitoramento. Paralelamente, a opção pela aquisição de um ADC visa otimizar o desempenho do tráfego interno da infraestrutura de TI e garantindo alta disponibilidade das aplicações. Essa combinação estratégica proporciona uma solução balanceada entre custo e benefício, oferecendo alta performance, segurança e flexibilidade, adequadas ao crescimento e às demandas futuras da Administração Pública.

10.11.A implementação permitirá a substituição gradativa dos Citrix NetScaler, com transição assistida, testes de alta disponibilidade (RT-04), treinamento especializado (RT-05) e suporte técnico contínuo (RT-06), para ambas os lotes e as soluções escolhidas, assegurando continuidade do serviço e evolução tecnológica alinhada às necessidades do Tribunal. Espera-se ganho de eficiência operacional, aumento de resiliência e redução de riscos, eliminando dependência de soluções monolíticas e fortalecendo a infraestrutura híbrida do TJCE.

11. JUSTIFICATIVA DO PARCELAMENTO OU NÃO

11.1. Avaliada a possibilidade e a pertinência do parcelamento do objeto para atendimento da necessidade, considerando o tipo e o volume do objeto pretendido, a distribuição regional, bem como aspectos técnicos, operacionais e econômicos (inclusive economia de escala), identificou-se como melhor alternativa licitar em 2 (dois) lotes distintos, pelos seguintes motivos:

11.1.1. A natureza heterogênea das entregas (serviço em nuvem WAF × appliance ADC) recomenda a segregação para preservar especialização técnica e adequada alocação de riscos;

11.1.2. O parcelamento amplia a competitividade, evitando a reunião de objetos de forma restritiva ao mercado e permitindo a participação de fornecedores com perfis distintos;

11.1.3. A separação favorece governança e gestão contratual (SLAs, métricas e responsabilidades específicas por camada), com redução de riscos operacionais;

11.1.4. As estruturas de precificação são distintas (tráfego/consumo no WAF SaaS versus hardware/licenças/suporte no ADC), o que recomenda avaliação e disputa separadas para assegurar economicidade;

11.1.5. O arranjo modular permite evolução e manutenção independentes, com menor impacto sistêmico e maior continuidade do serviço;

11.1.6. O parcelamento é tecnicamente conveniente e economicamente vantajoso, sem perda relevante de economia de escala.

11.2. Restam, assim, distribuídos em proposta de divisão:

11.2.1. Lote 1 – Aquisição de appliance para solução balanceador de carga/controlador de entrega de aplicações (ADC) e serviços associados (suporte 24x7x365 e treinamento), conforme especificações técnicas do edital.

11.2.2. Lote 2 – Contratação de WAF como Serviço (SaaS), com franquia de tráfego e recursos de alta disponibilidade, baixa latência, proteção DDoS, proteção de APIs, DNSSEC, anti-bot, suporte 24x7x365, instalação/configuração e treinamento, nos termos do edital.

11.3. Nos termos dos arts. 47 a 49 da Lei Complementar nº 123/2006 e do art. 39 da Lei Estadual nº 15.306/2013, o tratamento diferenciado e simplificado às microempresas e empresas de pequeno porte deve ser concedido sempre que viável e vantajoso à Administração Pública, observadas as restrições legais e os princípios da eficiência, economicidade e continuidade do serviço público.

11.4. No caso presente, o valor estimado dos lotes supera o limite de R$ 80.000,00 (oitenta mil reais), estabelecido pelo art. 48, inciso I, da LC nº 123/2006, o que por si só afasta a hipótese de exclusividade de participação de ME/EPP.

11.5. Além disso, o objeto contempla duas soluções tecnológicas complementares, porém internamente indivisíveis dentro de cada lote, ambas estrategicamente críticas à

operação do Tribunal de Justiça do Estado do Ceará.

11.6. Cada lote processa todo o tráfego interno e externo do TJCE, configurando ponto único de trânsito de informações críticas, cuja operação demanda gestão técnica unificada e alta disponibilidade, não sendo viável o fracionamento ou subcontratação parcial por diferentes fornecedores sem comprometer a segurança cibernética, a integridade das informações e a continuidade dos serviços.

11.7. Ambas as soluções concentram e processam todo o tráfego interno e externo do TJCE, funcionando como pontos únicos de trânsito da informação e elementos centrais da infraestrutura crítica do Tribunal. Sua operação exige integração contínua, sincronização, métricas e políticas de segurança unificadas, fatores que impõem gestão técnica centralizada e interoperabilidade plena entre as camadas de segurança e entrega de aplicações.

11.8. A divisão ou reserva de cotas para ME/EPP — conforme prevista no art. 48, inciso III, da LC nº 123/2006, e art. 39, inciso III, da Lei Estadual nº 15.306/2013 — não se mostra tecnicamente aplicável nem vantajosa, por representar risco de fragmentação operacional, elevação de custos e prejuízo à integração e à confiabilidade do ambiente, enquadrando-se na exceção legal do art. 49, inciso III, da referida lei complementar, que admite o afastamento do tratamento diferenciado quando este "representar prejuízo ao conjunto ou complexo do objeto a ser contratado".

11.9. Ademais, o objeto envolve soluções de alta complexidade tecnológica, com exigência de certificações específicas de fabricante e suporte técnico especializado contínuo (24x7). Tais características tornam inviável o atendimento por fornecedores de pequeno porte sem comprometer o conjunto ou complexo do objeto, a eficiência operacional, a escalabilidade e a conformidade técnica do ambiente. Assim, a aplicação de reserva de cota ou de lote específico para ME/EPP não se mostra vantajosa nem tecnicamente exequível.

11.10. Assim, o afastamento do tratamento diferenciado para ME/EPP encontra-se devidamente motivado e amparado na legislação vigente, em razão da criticidade das soluções que concentram todo o tráfego interno e externo do Tribunal, da necessidade de gestão técnica unificada e da impossibilidade de execução por fornecedores distintos, preservando-se a disponibilidade, a segurança e a continuidade dos serviços essenciais prestados pelo Poder Judiciário Cearense.

12. DEMONSTRATIVO DE RESULTADOS PRETENDIDOS

12.1. A solução indicada permitirá o suprimento das necessidades, garantindo, ao menos em relação a este insumo, a não interrupção dos serviços de balanceamento de carga (ADC) e proteção de aplicações web (WAF), assegurando disponibilidade, desempenho e segurança dos sistemas institucionais do TJCE, inclusive os voltados ao público externo e à prestação jurisdicional.

12.2. A proposta — com desmembramento das funcionalidades de WAF e ADC em dois componentes — foi definida com base em critérios técnicos, operacionais e econômicos, priorizando economicidade, eficiência, eficácia e sustentabilidade (conforme análises da Seção 9). Essa abordagem otimiza recursos, reduz custos e garante maior especialização em cada camada. Os principais benefícios esperados são:

12.2.1. Eficiência operacional: O ADC por appliance dedicado assegura controle e desempenho na entrega de aplicações (balanceamento, terminação SSL/TLS, alta disponibilidade e integração com a infraestrutura existente), com governança por SLAs e melhor aproveitamento dos recursos já implantados.

12.2.2. Redução de custos (economicidade): a contratação do WAF como serviço (SaaS) e o licenciamento do ADC promovem racionalização do TCO ao longo da vigência, reduzindo despesas com manutenção de hardware, atualizações e suporte, além de mitigar dependência tecnológica indevida, conforme comparativos consolidados na Seção 9.

12.2.3. Evolução tecnológica: a separação entre segurança de aplicações (WAF) e entrega de aplicações (ADC) favorece adoção de tecnologias mais modernas e especializadas, atualizações contínuas e alinhamento a arquiteturas híbridas/multicloud, com menor impacto operacional e maior aderência a boas práticas.

12.2.4. Escalabilidade e disponibilidade: O WAF em nuvem oferece elasticidade e cobertura geográfica, com CDN e, quando aplicável, GSLB, melhorando desempenho e resiliência frente a DDoS e outras ameaças, especialmente em picos de demanda, enquanto o ADC mantém alta disponibilidade local e baixa latência aos serviços críticos.

12.2.5. Sustentabilidade e governança: A solução considera o ciclo de vida completo, com suporte 24x7, registros e relatórios para auditoria, integração com monitoramento/SIEM e aderência a normativos aplicáveis (Lei nº 14.133/2021, Res. CNJ 468/2022 e LGPD), mitigando riscos de obsolescência e fortalecendo a gestão de TIC do TJCE.

13. PROVIDÊNCIAS A SEREM ADOTADAS PELO TJCE

13.1. Para a execução e viabilidade da solução, não serão necessárias adequações físicas nos ambientes de trabalho ou obras civis no datacenter, uma vez que a infraestrutura existente é compatível e suficiente para a instalação e operação do ADC e para o consumo do WAF em nuvem. Permanecem, contudo, as seguintes condicionantes técnicas: disponibilidade de endereçamento IP e VLANs, portas e interfaces de rede compatíveis, certificados digitais institucionais atualizados, perfis de acesso administrativo, integração com ferramentas de monitoramento/SIEM e rotinas de backup de configuração.

13.2. Quanto à fiscalização e gestão contratual, o TJCE deverá designar formalmente gestor(es) e fiscal(is) do contrato, bem como equipe de apoio, observando a segregação de funções. A contratada proverá treinamento específico e transferência de conhecimento para a capacitação do corpo técnico, abrangendo operação, monitoramento, procedimentos de mudança, tratamento de incidentes e melhores práticas de segurança.

13.3. Para o WAF em SaaS (Lote 2), o TJCE deverá conduzir, com apoio da contratada, o onboarding controlado, compreendendo: (i) validação e eventual alteração de DNS e de certificados; (ii) definição e homologação de políticas de segurança (OWASP, APIs, anti-bot, DDoS) e listas de exceção; (iii) integração de logs e alertas ao SIEM institucional; (iv) estabelecimento de janelas de mudança, critérios de aceitação e plano de rollback; e (v) atualização da documentação técnica e dos playbooks operacionais.

13.4. Para o ADC por licenciamento (Lote 1), o TJCE deverá: (i) preparar ambiente de homologação; (ii) realizar migração assistida das configurações legadas, com testes de desempenho e alta disponibilidade (failover/preservação de sessão); (iii) alinhar SLA e métricas de monitoramento; (iv) registrar procedimentos de backup/restore e gestão de capacidade; e (v) atualizar diagramas, inventário e trilhas de auditoria.

13.5. Em matéria de conformidade e segurança, caberá ao TJCE assegurar a observância dos normativos aplicáveis (Lei nº 14.133/2021, LGPD, Resoluções do CNJ e PSI institucional), incluindo gestão de acessos, segregação de ambientes (produção/homologação), retenção de logs conforme política vigente, e registro documental das evidências de aceite, inspeções e auditorias.

13.6. Para garantir a continuidade do serviço, o TJCE deverá manter plano de gestão de riscos, calendário de manutenções programadas, testes periódicos de contingência, e acompanhamento mensal de indicadores (disponibilidade, desempenho, incidentes), promovendo as ações corretivas necessárias em conjunto com a contratada.

14. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

14.1. Não há contratações correlatas e/ou interdependentes.

15. DESCRIÇÕES DE POSSÍVEIS IMPACTOS AMBIENTAIS

15.1. Seguindo o Plano de Logística Sustentável do Poder Judiciário do Estado do Ceará – PLS-TJCE 2021-2026 – que é um normativo de planejamento que permite a institucionalização de práticas de sustentabilidade, visando, dentre outros objetivos, a racionalização de gastos e de consumo por meio da construção e análise de indicadores e metas.

15.2. A empresa deverá possuir a licenças ambientais condizentes com a sua atividade produtiva e estar em dia com as respectivas licenças;

15.3. Os produtos devem observar os critérios de sustentabilidade ambiental decorrentes de sua fabricação, nos termos da legislação de regência e suas eventuais alterações;

15.4. As empresas poderão comprovar (por outros meios de prova válidos e regulares admitidos pelo direito) que seus produtos atendem aos requisitos de sustentabilidade ambiental (Acórdão no. 508/2013 – TCU Plenário; Acórdão no. 2.403/2012 – TCU – Plenário; Acórdão no. 1.929/2013 – TCU – Plenário e Acórdão no. 1.666/2019 – TCU – Plenário).

15.5. Os resíduos decorrentes dos produtos cotados deverão ter destinação ambiental adequada, como coleta seletiva nas unidades do TJCE.

16. CLASSIFICAÇÃO DOS ESTUDOS TÉCNICOS PRELIMINARES

16.1. Não há necessidade de classificar estes Estudos Preliminares como sigilosos, nos termos da Lei nº 12. 527, de 2011 (Lei de Acesso à Informação).

17. LEGISLAÇÃO APLICÁVEL AO OBJETO

17.1. O tipo de solução identificada como mais adequada para atendimento da necessidade, atrai a incidência das seguintes normas e diretrizes específicas, que devem ser observadas na implementação da solução:

17.1.1. Lei nº 14.133, de 1º de abril de 2021, Lei de Licitações e Contratos Administrativos, que disciplina a contratação pública de bens e serviços;

17.1.2. Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), considerando o tratamento de dados trafegados;

17.1.3. Resolução CNJ nº 468/2022, que dispõe sobre diretrizes para contratações de soluções de TIC pelos órgãos do Poder Judiciário, com ênfase em soluções em nuvem e segurança da informação;

17.1.4. ABNT NBR ISO/IEC 27001: Sistema de Gestão de Segurança da Informação, aplicável à empresa contratada e aos serviços prestados;

17.1.5. ABNT NBR ISO/IEC 27002: Código de boas práticas para controles de segurança da informação, como referência para os requisitos mínimos de proteção aplicáveis ao serviço WAF;

17.1.6. ABNT ISO/IEC 27017: Diretrizes de segurança da informação específicas para serviços em nuvem;

17.1.7. ABNT ISO/IEC 27018: Práticas de proteção de dados pessoais em ambientes de computação em nuvem;

17.1.8. Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), com foco na garantia da privacidade e segurança das informações trafegadas em rede;

17.1.9. Instruções Normativas da Secretaria de Governo Digital e orientações do Tribunal de Contas da União (TCU) relativas à contratação de soluções SaaS e computação em nuvem;

17.1.10. Política Nacional de Segurança da Informação (Decreto nº 10.222/2020), no que couber à proteção de ativos de informação do Estado;

17.1.11. Normativos internos do CNJ e do TJCE, que tratem de governança de TIC, segurança da informação e contratação de soluções em nuvem;

17.1.12. Quaisquer outras normas técnicas ou regulamentações nacionais e internacionais aplicáveis à contratação, prestação e gestão de serviços na nuvem, incluindo as obrigações da contratada quanto à conformidade, privacidade, segurança, SLA e disponibilidade.

18. POSICIONAMENTO CONCLUSIVO

18.1. Com base nas informações levantadas ao longo deste Estudo Técnico Preliminar, foi identificada solução viável de prosseguir e ser concretizada para atendimento da necessidade, na medida em que:

18.1.1. A necessidade apontada é clara e adequadamente justificada;

18.1.2. O atendimento está alinhado com os objetivos estratégicos do órgão e com os programas/atividades inerentes ao TJCE;

18.1.3. As quantidades estão coerentes com os requisitos quantitativos e qualitativos que precisam ser atendidos para resolução da necessidade identificada;

18.1.4. A análise de opções demonstra haver forma de atender ao suprimento demandado.

18.2. Os resultados pretendidos com solução escolhida atendem aos requisitos apresentados e agregam ganhos de eficiência administrativa;

18.3. Foram realizadas estimativas expeditas de preços de mercado, a fim de que se permita avaliar, aprovar e programar o provimento dos recursos necessários ao longo de todo o período de implantação da solução e os valores estimados mostram-se razoáveis e coerentes ao que a solução abrange;

18.4. Diante do exposto, indica-se como viável e recomendado a contratação da Solução A – WAF em nuvem como Serviço (SaaS) e da Solução C - Licenciamento (ADC).

Fortaleza, na data da assinatura eletrônica

Equipe de Planejamento:

Francisco José Pessoa Furtado - 8284

INTEGRANTE ADMINISTRATIVO

Matheus Freire e Silva do Nascimento - 50707

INTEGRANTE DEMANDANTE

Max Eduardo Vizcarra Melgar - 48994

INTEGRANTE TÉCNICO

Documento assinado eletronicamente por **MAX EDUARDO VIZCARRA MELGAR**, **Gestor de Unidade**, em 20/04/2026, às 14:33, conforme horário oficial de Brasília, com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015 .

Documento assinado eletronicamente por **MATHEUS FREIRE E SILVA DO NASCIMENTO**, **Gestor de Unidade**, em 20/04/2026, às 14:42, conforme horário oficial de Brasília, com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015 .

Documento assinado eletronicamente por **FRANCISCO JOSÉ PESSOA FURTADO**, **Gestor de Unidade**, em 20/04/2026, às 14:46, conforme horário oficial de Brasília, com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015 .

A autenticidade deste documento pode ser conferida no site https://sei-adm.tjce.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0603623** e o código CRC **76CE00AE**.

Referência: Processo nº 8515550-95.2025.8.06.0000 SEI nº 0603623