ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
COORDENADORIA DE CIBERSEGURANÇA

TERMO DE REFERÊNCIA

Síntese do Tipo de Demanda: Contratação de solução para balanceamento de carga e proteção de aplicações web do TJCE, contemplando fornecimento de equipamentos, implantação, configuração, suporte técnico, treinamento e disponibilização de serviço em modelo Software como Serviço (SaaS).

Código da Contratação: AQSETIN2025003 - Solução de balanceamento de carga e WAF

1. OBJETO DA CONTRATAÇÃO

1.1. O presente Termo de Referência tem por objeto a contratação de solução de balanceamento de carga e proteção de aplicações web, compreendendo a aquisição de Controlador de Entrega de Aplicações (Application Delivery Controller – ADC) em appliance físico, incluindo hardware, software e licenciamento em caráter perpétuo, com garantia de 60 (sessenta) meses, bem como serviços de instalação/configuração, suporte técnico especializado contínuo e treinamento da solução (LOTE 1); e prestação de serviços de Firewall de Aplicação Web (Web Application Firewall – WAF), na modalidade Software como Serviço (SaaS) contínuo, pelo período de 36 (trinta e seis) meses, incluindo subscrição, implantação, configuração e suporte técnico especializado (LOTE 2), conforme especificações e quantidades estabelecidas neste Termo de Referência, observadas as condições definidas nos ANEXOS I e II deste documento, com vistas a garantir a disponibilidade, a segurança e o desempenho dos serviços digitais do Tribunal de Justiça do Estado do Ceará (TJCE).

1.2. A solução a ser contratada é composta por duas camadas que apresentam características técnicas, modelos de fornecimento e mercados fornecedores distintos. Em razão disso, e com o objetivo de ampliar a competitividade do certame e permitir a participação de fornecedores especializados em cada tecnologia, a contratação será estruturada em dois lotes:

Lote 1			
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QUANTIDADE**
1	Controlador de Entrega de Aplicações (ADC)	Unidade	02
2	Suporte	Mês	57
3	Treinamento	Alunos	08
4	Instalação	Unidade	02

Lote 2

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	Web Application Firewall (WAF) em modelo Software como Serviço (SaaS), com franquia mensal de 50 TB de tráfego inspecionado	Mês	36
2	Franquia adicional de tráfego inspecionado a ser consumido e contratado sob demanda durante a vigência contratual	TB	900
3	Proteção DNS para 1 zona	Mês	36

1.3. Os quantitativos indicados neste Termo de Referência são estimativos e foram definidos com base nas análises constantes no Estudo Técnico Preliminar, não gerando obrigação de contratação ou pagamento por quantidades não solicitadas.

1.4. Os bens e serviços objeto da contratação são caracterizados como comuns, uma vez que possuem padrões de desempenho e qualidade objetivamente definidos no mercado, sendo comparáveis entre diferentes fornecedores mediante especificações usuais, conforme justificativa constante no Estudo Técnico Preliminar.

1.5. Em caso de divergência entre o descritivo dos itens constante deste Termo de Referência e quaisquer outros documentos relacionados à contratação, inclusive anexos ou sistemas eletrônicos utilizados para a realização do certame, prevalecerá o descritivo estabelecido neste Termo de Referência.

1.6. A presente contratação envolve fornecimento e serviços de natureza distinta, sendo:

1.6.1. Lote 1 – aquisição de solução ADC em appliance físico, com fornecimento de equipamento, licenciamento perpétuo e serviços associados (suporte técnico e garantia), cuja execução possui caráter pontual na entrega, porém com obrigações acessórias de natureza continuada durante a vigência contratual, especialmente no que se refere ao suporte técnico e manutenção evolutiva da solução (item 2 do Lote 1);

1.6.2. Lote 2 – contratação de solução de Web Application Firewall (WAF) no modelo Software como Serviço (SaaS), caracterizando-se como serviço contínuo, essencial à manutenção da segurança das aplicações web do TJCE, cuja interrupção pode comprometer a disponibilidade, integridade e confidencialidade dos sistemas institucionais, configurando necessidade administrativa permanente.

1.6.3. Dessa forma, a contratação, no que se refere à prestação de serviços de suporte técnico (Lote 1) e ao serviço em nuvem (Lote 2), enquadra-se como de natureza continuada, nos termos do art. 6º, inciso XV, da Lei nº 14.133/2021.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. A contratação permitirá que o TJCE disponha de solução moderna e eficiente para balanceamento de carga e proteção de aplicações web, com recursos avançados de distribuição de tráfego, otimização de desempenho e mitigação de ataques, assegurando a proteção e a estabilidade das aplicações críticas do TJCE. A solução está alinhada aos objetivos estratégicos institucionais de celeridade, segurança da informação e transformação digital.

2.2. Conforme detalhado no Estudo Técnico Preliminar (ETP), a solução pretendida é essencial à manutenção das atividades do TJCE, por estar diretamente relacionada à infraestrutura crítica de Tecnologia da Informação, indispensável à continuidade da prestação jurisdicional e administrativa. A solução visa substituir os atuais equipamentos Citrix NetScaler, cuja ausência de suporte técnico e limitações de desempenho comprometem a segurança e a disponibilidade dos serviços digitais do Tribunal.

2.3. A solução adotada é composta por camadas tecnológicas complementares e interoperáveis, estruturadas de forma a garantir especialização funcional e desempenho adequado das aplicações web. Nesse contexto, o Controlador de Entrega de Aplicações (ADC) atua na distribuição, disponibilidade e otimização do tráfego, enquanto o Web Application Firewall (WAF) concentra-se na proteção das aplicações contra ameaças cibernéticas.

2.4. A adoção de arquitetura baseada em componentes independentes e desacoplados favorece a evolução tecnológica, a realização de manutenções com menor impacto operacional e a mitigação de riscos de indisponibilidade, além de permitir maior flexibilidade na adaptação ao ambiente híbrido do TJCE, composto por infraestrutura local e serviços em nuvem.

2.5. O componente de proteção de aplicações web (WAF) será contratado no modelo Software como Serviço (SaaS), caracterizado por prestação contínua em nuvem, escalabilidade sob demanda, atualização tecnológica permanente e suporte técnico especializado, garantindo a sustentação operacional contínua das aplicações institucionais.

2.6. A solução adotada é composta por camadas tecnológicas complementares e interoperáveis, estruturadas de forma a garantir especialização funcional e desempenho adequado das aplicações web. Nesse contexto, o Controlador de Entrega de Aplicações (ADC) atua na distribuição, disponibilidade e otimização do tráfego, enquanto o Web Application Firewall (WAF) concentra-se na proteção das aplicações contra ameaças cibernéticas.

2.7. A solução deverá ser considerada ao longo de todo o seu ciclo de vida, abrangendo as fases de implantação, operação, manutenção e evolução tecnológica, de forma a garantir a continuidade, disponibilidade e segurança dos serviços digitais do TJCE, incluindo:

2.7.1. implantação, com instalação, configuração, integração com o ambiente existente e entrada em operação assistida;

2.7.2. operação contínua da solução, com monitoramento e suporte técnico especializado;

2.7.3. manutenção corretiva, preventiva, adaptativa e evolutiva;

2.7.4. fornecimento contínuo de atualizações de software, assinaturas de segurança e suporte técnico durante toda a vigência contratual;

2.7.5. evolução da solução, com possibilidade de ampliação de capacidade e adequação a novos cenários tecnológicos.

2.8. **Bens e serviços que compõem a solução:**

2.8.1. Lote 1: Aquisição de Controlador de Entrega de Aplicações (ADC) em appliance físico, incluindo hardware, software, licenciamento e serviços associados (suporte 24x7x365, configuração, instalação e treinamento remoto);

2.8.2. Lote 2: Contratação de serviço de Web Application Firewall (WAF) no modelo Software como Serviço (SaaS), incluindo licenciamento, configuração, migração assistida, suporte técnico 24x7x365 e garantia de atualização contínua da solução.

3. JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. A contratação do objeto deste Termo de Referência visa substituir os atuais equipamentos Citrix NetScaler e garantir a disponibilidade, o desempenho e a segurança das aplicações web críticas do TJCE, conforme demonstrado nos Estudos Técnicos Preliminares.

3.2. **Contextualização e justificativa da contratação**

3.2.1. Atualmente, a Secretaria de Tecnologia da Informação do TJCE utiliza, em sua infraestrutura, solução de balanceamento de carga e segurança de aplicações web baseada em equipamentos e softwares Citrix NetScaler, conforme detalhamento a seguir:

3.2.1.1. 02 (dois) equipamentos Citrix NetScaler SDX 8920HB SE Hardware (6x10/100/1000 e 4x10GE BASE-X SFP+);

3.2.1.2. 04 (quatro) módulos Citrix NetScaler SFP 10 Gigabit Ethernet Short Range 300m;

3.2.1.3. 02 (dois) módulos Citrix NetScaler Power Supply, 450W AC;

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

3.2.2. Verifica-se que a solução atualmente em uso encontra-se em processo de obsolescência tecnológica, com limitações de desempenho, ausência de suporte técnico ativo e restrições quanto à evolução e atualização da plataforma, o que compromete a segurança, a disponibilidade e a eficiência dos serviços digitais do Tribunal.

3.2.3. Nesse contexto, a manutenção da solução atual representa risco operacional relevante, podendo ocasionar indisponibilidade dos sistemas institucionais, exposição a vulnerabilidades de segurança e degradação do desempenho das aplicações críticas, impactando diretamente a prestação jurisdicional e administrativa.

3.2.4. A solução proposta, conforme definida no Estudo Técnico Preliminar, baseia-se na adoção de arquitetura em camadas complementares, composta por Controlador de Entrega de Aplicações (ADC) e Web Application Firewall (WAF), permitindo especialização funcional, maior eficiência operacional, evolução tecnológica independente e mitigação de riscos de indisponibilidade e de segurança cibernética.

3.2.5. O Controlador de Entrega de Aplicações (ADC) desempenha papel fundamental na distribuição, disponibilidade e otimização do tráfego das aplicações institucionais, atuando como o primeiro ponto de recepção das requisições destinadas às aplicações do TJCE. Nesse contexto, é responsável pelo balanceamento de carga entre os servidores de back-end, gerenciamento de conexões e garantia de alta disponibilidade, assegurando a distribuição eficiente das requisições, evitando sobrecarga nos servidores e contribuindo diretamente para a redução de latência, aumento do desempenho e resiliência dos sistemas críticos.

3.2.6. O Web Application Firewall (WAF), por sua vez, concentra-se na proteção das aplicações web contra ameaças cibernéticas, incluindo ataques a vulnerabilidades conhecidas, tráfego malicioso automatizado e exploração de interfaces de integração. Atua de forma complementar aos mecanismos tradicionais de segurança de borda (firewall), oferecendo abordagem especializada na camada de aplicação, capaz de inspecionar e tratar requisições HTTP/HTTPS de forma mais granular e contextualizada. A solução será adotada no modelo Software como Serviço (SaaS), o que possibilita escalabilidade sob demanda, atualização contínua e maior aderência a ambientes híbridos (on-premises e nuvem).

3.2.7. A solução a ser contratada deverá contemplar:

3.2.7.1. suporte técnico especializado contínuo (24x7x365);

3.2.7.2. atualização permanente de software e assinaturas de segurança de forma contínua;

3.2.7.3. proteção contra ameaças cibernéticas, incluindo OWASP Top 10, ataques DDoS, bots e proteção de APIs;

3.2.7.4. alta disponibilidade e escalabilidade da infraestrutura de forma contínua;

3.2.7.5. aderência ao ciclo de vida do objeto, com manutenção corretiva, preventiva, adaptativa e evolutiva de forma contínua.

3.2.8. Considerando a necessidade permanente de sustentação dos serviços digitais do Tribunal, a interrupção ou degradação da solução pode comprometer o acesso aos sistemas judiciais eletrônicos, afetar a prática de atos processuais, prejudicar a comunicação institucional e expor aplicações a riscos de segurança. O objeto caracteriza-se como serviço contínuo, nos termos do art. 6º, XV, da Lei nº 14.133/2021, por atender a necessidade permanente da Administração, sendo indispensável à manutenção das atividades institucionais.

3.2.9. A solução atende a necessidade permanente da Administração, sendo essencial à sustentação dos serviços digitais do TJCE, envolvendo, de forma indissociável, o fornecimento de infraestrutura e a prestação de serviços de suporte técnico, manutenção e atualização contínua.

3.2.10. A presente contratação decorre de demanda formalizada no Documento de Oficialização da Demanda (DOD) e analisada no Estudo Técnico Preliminar (ETP), que identificaram a necessidade de modernização da infraestrutura tecnológica e a mitigação dos riscos operacionais associados à solução atualmente em uso.

3.3. **Alinhamento aos instrumentos de planejamento institucionais**

3.3.1. A contratação ora pretendida está em consonância com os objetivos estratégicos do Plano de Contratações de STIC 2025, alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2025/2027, ao Planejamento Estratégico Institucional 2021/2030, bem como à Estratégia Nacional do Poder Judiciário e à Estratégia Nacional de TIC (ENTIC-JUD). O objeto contempla a aquisição de uma solução de balanceamento de carga e segurança para aplicações web, capaz de realizar a distribuição uniforme do tráfego entre servidores, otimizar a performance, garantir baixa latência, proteger contra ameaças cibernéticas, realizar inspeção do tráfego HTTP e bloquear tentativas de ataques. A medida assegura a integridade e a confidencialidade dos dados processados pelas aplicações web, fortalece a infraestrutura tecnológica do Tribunal, reforça a segurança da informação e garante a continuidade dos serviços digitais, fatores imprescindíveis para o pleno funcionamento do TJCE no desempenho de suas atividades institucionais.

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

3.3.3. Destaca-se, ainda, que o movimento de evolução do modelo de TIC do TJCE alinha-se às melhores práticas de governança de TI, especialmente ao adotar critérios, métricas e controles mais rigorosos de mensuração dos serviços prestados.

3.4. **Estimativa da demanda**

3.4.1. As quantidades estimadas da demanda encontram-se detalhadas no Estudo Técnico Preliminar.

3.5. **Parcelamento da solução de TIC**

3.5.1. Avaliando a possibilidade e a pertinência do parcelamento do objeto para atendimento da necessidade, considerou-se o tipo e volume do objeto pretendido e a distribuição regional, assim como os aspectos técnicos, operacionais e econômicos, sobretudo de economia de escala e custos com transporte e respectiva amortização, de modo que resultou na identificação de melhor opção em licitar em 02 (dois) diferentes lotes, pois essa divisão permite segregar de forma adequada os componentes da solução (equipamento/licenciamento e serviços em nuvem), garantindo maior competitividade, especialização dos fornecedores e aderência ao mercado, sem prejuízo à economicidade. A solução resta assim distribuída:

3.5.1.1. Lote 1 – Aquisição de Controlador de Entrega de Aplicações (ADC) em appliance físico,

incluindo hardware, software, licenciamento e serviços associados (suporte 24x7x365, configuração, instalação e treinamento remoto);

3.5.1.2. Lote 2 – Contratação de WAF Software como Serviço (SaaS) e serviços associados (suporte 24x7x365, garantia, licenciamento, instalação, configuração e treinamento);

3.5.2. A solução será contratada de forma parcelada em lotes distintos, considerando que os componentes tecnológicos envolvidos (ADC e WAF) possuem naturezas, modelos de fornecimento e mercados fornecedores distintos.

3.5.3. A divisão em lotes mostra-se tecnicamente adequada, considerando que a solução de WAF em nuvem é capaz de atender, de forma integrada, tanto ambientes on-premises quanto ambientes em nuvem, enquanto a solução de ADC possui natureza distinta, voltada à infraestrutura local.

3.5.4. A adoção de lote único poderia restringir a competitividade, ao limitar a participação de fornecedores que não atuam em todos os componentes da solução.

3.5.5. O parcelamento atende aos requisitos técnicos e de negócio definidos no Estudo Técnico Preliminar (ETP), além de ampliar a competitividade e assegurar a obtenção da proposta mais vantajosa para a Administração.

3.6. **Resultados e benefícios a serem alcançados**

3.6.1. A solução indicada atenderá às necessidades institucionais de balanceamento de carga e proteção das aplicações web do Tribunal de Justiça do Estado do Ceará (TJCE), contribuindo para ampliar a disponibilidade, o desempenho e a segurança dos serviços digitais utilizados por magistrados, servidores e pela sociedade.

3.6.2. Esses serviços sustentam atividades essenciais à prestação jurisdicional, como o acesso a sistemas processuais eletrônicos, portais institucionais e outras aplicações críticas do Tribunal. Nesse contexto, a adoção da solução contribui para reduzir riscos de indisponibilidade, mitigar ameaças cibernéticas e garantir a continuidade operacional do ambiente tecnológico do TJCE.

3.6.3. No âmbito da entrega de aplicações, a solução atuará como componente estratégico da infraestrutura de acesso aos serviços digitais do Tribunal, realizando o balanceamento e a distribuição das requisições entre os ambientes de processamento. Essa capacidade permite absorver variações de demanda, melhorar o desempenho das aplicações e aumentar a resiliência dos serviços diante de falhas ou degradações de infraestrutura.

3.6.4. No aspecto da segurança, a solução também desempenhará papel relevante na proteção do tráfego direcionado às aplicações institucionais, por meio de mecanismos de inspeção e mitigação de ameaças próprios de Web Application Firewall (WAF). Com isso, busca-se reduzir riscos associados à exploração de vulnerabilidades em aplicações expostas à internet e fortalecer a proteção do ambiente tecnológico do Tribunal.

3.6.5. Com essas capacidades, a solução contribui para assegurar a continuidade e a confiabilidade dos serviços digitais que apoiam a atividade-fim do Poder Judiciário, evitando interrupções que possam comprometer o acesso à informação processual, a prática de atos processuais eletrônicos e a comunicação entre o Tribunal e os demais atores do sistema de justiça, preservando ao mesmo tempo uma adequada relação custo-benefício para a Administração Pública.

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. **Condições gerais para execução da contratação**

4.1.1. A **CONTRATADA** deverá possuir aptidão técnica e operacional para a execução dos serviços previstos neste Termo de Referência, em características, quantidades e prazos compatíveis com o objeto da contratação.

4.1.2. Capacidade e disponibilidade para emitir notas fiscais de serviços.

4.1.3. A **CONTRATADA** deve alocar nas atividades somente trabalhadores com vínculos formais e necessariamente segurados do Instituto Nacional do Seguro Social.

4.1.4. A **CONTRATADA** deverá utilizar somente as formas juridicamente válidas para a vinculação dos trabalhadores e promover sua gestão de modo responsável, com atendimento pleno das normas e direitos trabalhistas e prevenção de riscos e acidentes de trabalho;

4.1.5. Nos casos de atividades, ou parte delas, controladas ou de exercício mediante autorização prévia, caberá à **CONTRATADA** a regularização e obtenção de respectiva(s) licença(s) ou registro(s);

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

4.1.6.1. 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;

4.1.6.2. Não ter sido condenada, a **CONTRATADA** 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;

4.1.7. A **CONTRATADA** deverá comprovar, no início da prestação dos serviços e a cada prorrogação contratual, o cumprimento da política de empregabilidade estabelecida no art. 93 da Lei no 8.213/1991.

4.2. **Requisitos de negócio**

4.2.1. Considerando as necessidades do negócio relacionadas aos sistemas e às soluções de informação do TJCE, destacam-se os seguintes recursos e funcionalidades:

4.2.2. 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 24x7x365, 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.

4.3. **Requisitos de capacitação**

4.3.1. Os profissionais deverão receber capacitações técnicas e comportamentais pela CONTRATADA para as atividades a serem desenvolvidas, podendo ainda receber treinamentos de ambientação e conhecimentos específicos de particularidades do TJCE, por este promovidos.

4.3.2. O treinamento mínimo obrigatório deverá contemplar:

4.3.2.1. Carga horária: 24 (vinte e quatro) horas;

4.3.2.2. Modalidade: remota (síncrona);

4.3.2.3. Participantes: até 08 (oito) integrantes da equipe técnica do TJCE;

4.3.2.4. Conteúdo: configuração, operação, monitoramento e solução de incidentes relacionados à solução de ADC e WAF contratada;

4.3.2.5. Materiais didáticos: deverão ser fornecidos pela CONTRATADA em meio digital;

4.3.2.6. Ambiente tecnológico: deverá ser assegurado pela CONTRATADA, compatível com as soluções contratadas.

4.3.3. As capacitações técnicas abrangerão conhecimentos específicos relacionados às atividades desempenhadas pelos empregados da **CONTRATADA**, com o objetivo de atualizá-los sobre práticas, normas, regulamentos e avanços relevantes em suas respectivas áreas de atuação.

4.3.4. As capacitações serão realizadas pela **CONTRATADA** de forma habitual e com comprovação formal ao TJCE (atas, certificados ou relatórios), facultando ao Tribunal propor ou acrescentar formações adicionais relacionadas às atividades.

4.4. **Requisitos legais**

4.4.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Resolução CNJ n.º 468/2022 e suas atualizações, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

4.4.2. Além dessas referências normativas, devem ser observados os ditames da Instrução Normativa SGD/ME nº 94/2022, que disciplina o processo de contratação de soluções de TIC, bem como

as diretrizes da Estratégia Nacional de TIC do Poder Judiciário (ENTIC-JUD) e demais normativos internos do TJCE e do CNJ relacionados à governança, segurança da informação e contratações públicas).

4.5. **Requisitos de manutenção**

4.5.1. Devido às características da solução, é obrigatória a garantia contratual e a realização de manutenções corretivas, preventivas, adaptativas e evolutivas pela **CONTRATADA**, de forma a assegurar a continuidade do fornecimento da solução de TIC em caso de falhas:

4.5.2. Manutenção corretiva: pronta resposta para a correção de falhas críticas ou degradação de desempenho que comprometam a disponibilidade dos serviços digitais;

4.5.3. Manutenção preventiva: aplicação de patches de segurança, atualizações de firmware e melhorias recomendadas pelo fabricante para prevenir vulnerabilidades e incidentes operacionais;

4.5.4. Manutenção adaptativa: adequações necessárias para manter a compatibilidade da solução com mudanças na infraestrutura de TI do TJCE, tais como integrações com novos sistemas ou migração para ambientes híbridos;

4.5.5. Manutenção evolutiva: incrementos de funcionalidades e melhorias de desempenho disponibilizadas pelo fabricante ou prestador SaaS, garantindo a atualização tecnológica contínua da solução de ADC e WAF.

4.5.6. As manutenções deverão ser executadas de modo a assegurar alta disponibilidade, baixa latência e resiliência da solução, sem impacto nas operações críticas do TJCE e em conformidade com as melhores práticas de mercado.

4.5.7. Inclui-se, nesse escopo, a prestação de suporte técnico especializado 24x7x365, atualizações contínuas de segurança, aplicação de melhorias tecnológicas, correções de falhas identificadas na operação da plataforma e ajustes de configuração decorrentes da evolução do ambiente do TJCE;

4.6. **Requisitos temporais do Lote 1**

4.6.1. O prazo máximo para a execução integral do objeto contratual será de 90 (noventa) dias corridos, contados da data de assinatura do contrato, compreendendo todas as atividades necessárias à completa entrega da solução.

4.6.2. A entrega dos equipamentos deverá ocorrer no prazo máximo de 60 (sessenta) dias corridos, contados a partir do recebimento da Ordem de Fornecimento de Bens (OFB) pela CONTRATADA.

4.6.3. Os equipamentos deverão ser entregues nos seguintes locais, no município de Fortaleza – CE, conforme indicado pela CONTRATANTE na Ordem de Fornecimento de Bens (OFB):

4.6.4. Tribunal de Justiça do Estado do Ceará, situado na Av. General Afonso Albuquerque Lima, s/n, Cambeba, CEP 60822-325.

4.6.5. Fórum Clóvis Beviláqua, situado na Rua Des. Floriano Benevides Magalhães, nº 220, Edson Queiroz, Fortaleza – CE, CEP 60811-690.

4.6.6. O prazo para execução das atividades de instalação física, configuração, integração, testes e operação assistida será de até 30 (trinta) dias corridos, contados da entrega dos equipamentos.

4.6.7. O início da prestação dos serviços de assistência técnica e suporte, bem como a contagem do prazo de 57 (cinquenta e sete) meses, ocorrerá no dia subsequente à emissão do Termo de

Recebimento Definitivo (TRD) da solução.

4.6.8. A solução fornecida deverá possuir garantia do fabricante pelo prazo mínimo de 60 (sessenta) meses, contados a partir da emissão do Termo de Recebimento Definitivo (TRD) da solução.

4.6.9. O prazo referente ao Treinamento será de 30 (trinta) dias corridos após a emissão, pelo Tribunal, de ordem de serviço, que ocorrerá após a emissão do Termo de Recebimento Definitivo (TRD) da solução.

4.6.10. Na execução dos serviços, deverão ser observados os seguintes prazos:

Atividade, Tarefa ou Serviço	**Prazo máximo**
Entrega dos equipamentos	até 60 dias corridos após emissão da OFB
Instalação física e energização dos equipamentos	até 30 dias corridos após emissão da OS
Configuração inicial e integração	
Documentação as-built	
Treinamento	até 30 dias corridos após emissão da OS
Suporte técnico especializado, Atendimento de incidente ou indisponibilidade da solução	57 Meses após emissão do TRD
Garantia do fabricante	60 Meses

4.7. **Requisitos temporais do Lote 2**

4.7.1. A disponibilização e ativação da solução de WAF em modelo Software como Serviço (SaaS) deverá ocorrer no prazo máximo de 75 (setenta e cinco) dias corridos, contados a partir do recebimento da Ordem de Serviço (OS) pela CONTRATADA.

4.7.2. Os serviços serão prestados de forma remota, por meio da infraestrutura da CONTRATADA, com proteção das aplicações web e serviços digitais disponibilizados pela CONTRATANTE, incluindo os ambientes hospedados em seu datacenter ou em infraestruturas de nuvem utilizadas pelo órgão.

4.7.2.1. Na execução dos serviços, deverão ser observados os seguintes prazos:

Atividade, Tarefa ou Serviço	**Prazo máximo**
Disponibilização e ativação da solução WAF após emissão da OS	até 75 dias corridos após emissão da OS
Onboarding inicial das aplicações protegidas	
Ajuste de regras de segurança ou políticas de proteção	

Documentação as-built	
Passagem de Conhecimento	
Suporte técnico especializado, Atendimento de incidente ou indisponibilidade da solução	36 Meses

4.7.3. Os prazos estabelecidos neste item representam limites máximos para execução das atividades. O descumprimento injustificado implicará a aplicação das sanções previstas no contrato.

4.7.4. Os prazos poderão ser ajustados mediante acordo formal entre o TJCE e a CONTRATADA, desde que devidamente justificado e registrado.

4.8. **Requisitos de segurança e privacidade**

4.8.1. Os requisitos de segurança deverão ser observados para cada lote da contratação, considerando as diretrizes estabelecidas na Política de Segurança da Informação (PSI), definida pela Resolução do Órgão Especial nº 15/2023, que garante a integridade, a confidencialidade e a disponibilidade das informações do Poder Judiciário do Estado do Ceará.

4.8.2. Lote 1 – Controlador de Entrega de Aplicações (ADC)

4.8.2.1. Implementação de balanceamento de carga seguro, com criptografia ponta a ponta (SSL/TLS) e compatibilidade com a infraestrutura de certificados digitais do TJCE.

4.8.2.2. Alta disponibilidade com mecanismos de failover automático e preservação de sessões ativas, assegurando a continuidade dos serviços críticos.

4.8.2.3. Geração e retenção de logs e trilhas de auditoria para rastreabilidade e investigação de incidentes.

4.8.2.4. Conformidade com a PSI, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e as normas de segurança definidas pelo CNJ.

4.8.3. Lote 2 – WAF como Serviço (SaaS)

4.8.3.1. Proteção contra ameaças cibernéticas, incluindo ataques listados no OWASP Top 10 e negação de serviço (DDoS).

4.8.3.2. Proteção de APIs com autenticação, limitação de taxa (rate limiting), inspeção de payload e bloqueio de ataques conhecidos.

4.8.3.3. Mitigação de bots (anti-bot), suporte a DNSSEC e prevenção contra injeções e exploração de vulnerabilidades em tempo real.

4.8.3.4. Relatórios de segurança, monitoramento contínuo e alertas automáticos para a equipe técnica do TJCE.

4.8.3.5. Conformidade com a PSI, as normas do CNJ e a Estratégia Nacional de Segurança Cibernética.

4.8.4. Requisitos Comuns aos Dois Lotes

4.8.4.1. Suporte 24x7x365 para incidentes e aplicação de patches de segurança de forma contínua;

4.8.4.2. Integração com as ferramentas de SIEM e monitoramento já existentes no TJCE;

4.8.4.3. Implementação de políticas de segurança padronizadas para ambos os ambientes, on-premises e nuvem, assegurando a uniformidade na proteção dos ativos digitais;

4.8.4.4. Estar em conformidade com as normas ISO/IEC 27001 e 27002;

4.8.4.5. Suportar criptografia de tráfego SSL/TLS com inspeção e terminação segura;

4.8.4.6. Permitir a aplicação de políticas de controle de acesso e autenticação forte;

4.8.4.7. Garantir a rastreabilidade das ações por meio de logs e auditorias;

4.9. **Requisitos sociais, ambientais e culturais**

4.9.1. Os equipamentos devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

4.9.2. Observância de critérios de sustentabilidade ambiental, como uso de materiais recicláveis, eficiência energética e descarte adequado de resíduos eletrônicos;

4.9.3. Conformidade com o Plano de Logística Sustentável do TJCE (PLS-TJCE 2021–2026), promovendo a racionalização de recursos e a responsabilidade socioambiental.

4.9.4. Dessa forma, a PRESTADORA DE SERVIÇOS não apenas se compromete com a sustentabilidade ambiental, mas também com o bem-estar da sociedade, cumprindo requisitos que abrangem tanto aspectos ecológicos quanto sociais.

4.10. **Requisitos de arquitetura tecnológica**

4.10.1. Os equipamentos e serviços deverão observar integralmente os requisitos de arquitetura tecnológica estabelecidos pelo TJCE, garantindo integração e conformidade com os padrões de TIC da instituição.

4.10.2. A solução deverá possuir capacidade de integração com os sistemas existentes do TJCE, incluindo autenticação mútua por certificado digital, gerenciamento centralizado e interoperabilidade com soluções de segurança e monitoramento já implantadas.

4.10.3. Para o Lote 1 – Controlador de Entrega de Aplicações (ADC):

4.10.3.1. Compatibilidade com os sistemas e aplicações críticas hospedados no datacenter do TJCE;

4.10.3.2. Suporte a aplicações que utilizam recurso de virtualização ou execução em contêineres, conforme a política tecnológica do TJCE;

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;

4.10.3.4. Capacidade de operação em arquitetura redundante e de alta disponibilidade, garantindo recuperação automática em caso de falhas.

4.10.3.4.1.1. Deverá possuir interfaces compatíveis com a topologia do TJCE, sendo aceitas combinações equivalentes que suportem throughput ≥ 80 Gbps e agregação LACP.

4.10.3.4.1.2. A solução deverá ser capaz de atender ao throughput mínimo de 30 Gbps em camada L7.

4.10.4. Para o Lote 2 – WAF como Serviço (SaaS):

4.10.4.1. Disponibilidade em arquitetura distribuída e escalável, garantindo baixa latência e mitigação de pontos únicos de falha;

4.10.4.2. Integração via APIs e protocolos padrão para troca de informações com as plataformas internas do TJCE, incluindo autenticação federada quando aplicável;

4.10.4.3. Conformidade com padrões de nuvem híbrida e multi-cloud, permitindo flexibilidade na implantação e escalabilidade sob demanda;

4.10.4.4. Suporte a DNSSEC, proteção de APIs, mitigação de bots e mecanismos de segurança integrados conforme as diretrizes da PSI – Política de Segurança da Informação.

4.11. **Requisitos de projeto e de implementação**

4.11.1. Os equipamentos deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir:

4.11.2. Para o Lote 1 – Controlador de Entrega de Aplicações (ADC);

4.11.2.1. O projeto deverá incluir plano de instalação e configuração detalhado, contemplando integração com a infraestrutura existente e a topologia de rede do TJCE;

4.11.2.2. A implementação deverá ocorrer em ambiente redundante e de alta disponibilidade, garantindo que o balanceamento de carga não seja ponto único de falha;

4.11.2.3. Todas as atividades deverão ser realizadas com janelas de manutenção programadas e em conformidade com os procedimentos de segurança da PSI;

4.11.2.4. Deverá ser entregue documentação técnica completa, incluindo arquitetura, fluxos de tráfego, procedimentos de backup e recuperação, bem como estratégias de rollback.

4.11.3. Para o Lote 2 – WAF como Serviço (SaaS):

4.11.3.1. A implementação deverá prever onboarding seguro, com integração aos sistemas do TJCE sem interromper serviços existentes;

4.11.3.2. Deverá garantir baixa latência e alta escalabilidade, conforme níveis de serviço estabelecidos no contrato;

4.11.3.3. Serão exigidos testes de aceitação contemplando regras de segurança, proteção de APIs, mitigação de bots, DNSSEC e OWASP Top 10;

4.11.3.4. O fornecedor deverá disponibilizar manuais de operação, acesso ao painel de gerenciamento e treinamento remoto para a equipe técnica, conforme já descrito nos requisitos de capacitação.

4.12. **Requisitos de implantação**

4.12.1. A implantação da solução deverá seguir plano detalhado, aprovado previamente pela área técnica do TJCE, contendo cronograma, atividades, responsáveis, janelas de manutenção e pontos de verificação para garantir a execução ordenada e sem interrupções indevidas dos serviços:

4.12.2. Para o Lote 1 – Controlador de Entrega de Aplicações (ADC):

4.12.2.1. Instalação física em ambiente de homologação, considerando que a solução deve ser entregue exclusivamente em appliance físico, devido à exigência de 30 Gbps de throughput L7;

4.12.2.2. Integração com a topologia de rede existente e com as soluções de segurança e monitoramento já implantadas;

4.12.2.2.1.1. Migração assistida da configuração atual dos equipamentos Citrix NetScaler para a nova solução, com garantia de continuidade operacional e validação funcional pós-implantação;

4.12.2.3. Testes de alta disponibilidade, failover automático e preservação de sessões ativas antes da entrada em operação definitiva;

4.12.2.3.1. Entrega de relatório técnico de implantação, incluindo documentação de configuração, diagramas atualizados e registros de testes realizados.

4.12.2.4. Para o Lote 2 – WAF como Serviço (SaaS):

4.12.2.5. Processo de onboarding remoto, com credenciais seguras, configuração inicial e integração com os serviços críticos do TJCE;

4.12.2.6. Provisionamento de políticas de segurança alinhadas à Política de Segurança da Informação (PSI) e validação com a equipe técnica do TJCE;

4.12.2.7. Testes funcionais abrangendo mitigação de DDoS, proteção de APIs, anti-bot, DNSSEC e prevenção de ataques listados no OWASP Top 10;

4.12.2.8. Emissão de relatório de aceitação documentando os critérios atendidos e eventuais pendências corrigidas antes do aceite final.

4.13. **Critérios de Aceitação:**

4.13.1. Todos os serviços deverão ser validados pela equipe técnica do TJCE com checklists formais;

4.13.2. A solução somente será considerada entregue após a homologação final e a verificação de que todos os requisitos técnicos, funcionais e de segurança foram atendidos;

4.13.3. A fase de implantação deverá contemplar treinamento remoto para a equipe técnica, conforme carga horária e conteúdos descritos na seção de capacitação.

4.13.4. Instalação física e lógica da solução nos datacenters do TJCE, com configuração inicial realizada por equipe especializada da CONTRATADA;

4.14. **Requisitos de garantia, Manutenção e Assistência Técnica**

4.14.1. O prazo de garantia contratual dos bens, complementar e não menor que a garantia legal, será de:

4.14.1.1. 60 (sessenta) meses para o Lote 1 – Controlador de Entrega de Aplicações (ADC);

4.14.1.2. 36 (trinta e seis) meses para o Lote 2 – WAF como Serviço (SaaS);

4.14.1.3. Contados a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

4.14.2. A garantia será prestada com vistas a manter os objetos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o TJCE.

4.14.3. A garantia abrange a realização da manutenção corretiva, preventiva, adaptativa e evolutiva dos serviços pela própria CONTRATADA, com atendimento 24x7x365 para incidentes críticos.

4.14.4. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados nos serviços, compreendendo, caso couber, a substituição de peças, a realização de ajustes, reparos e correções necessárias e mesmo substituição de produtos, materiais ou insumos que se mostrem

impróprios ou sem condições de utilização.

4.14.5. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

4.14.6. Uma vez notificado, o Contratado realizará a reparação ou substituição dos itens que apresentarem vício ou defeito no prazo de até 7 (sete) dias, contados a partir da data de recebimento da notificação.

4.14.7. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado, a exclusivo critério do TJCE.

4.14.8. Decorrido o prazo para reparos e substituições, sem o atendimento da solicitação do TJCE e sem apresentação de justificativa plausível pela **CONTRATADA**, fica o TJCE autorizado a contratar **CONTRATADA** diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir da **CONTRATADA** o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos e sem prejuízo da aplicação de penalidades à **CONTRATADA** por descumprimento do compromisso de garantia.

4.14.9. Os custos incorridos na contratação de terceiros e na substituição de peças ou materiais, por decorrência de garantia não atendida no prazo notificado, serão devidos e cobrados a **CONTRATADA** que desatendeu ao prazo de atendimento da garantia.

4.14.10. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

4.14.11. O desatendimento do prazo e providências de garantia determina adicionalmente a aplicação de penalidade administrativa à **CONTRATADA**, na medida em que configura descumprimento de contrato.

4.15. **Requisitos de qualificação profissional**

4.15.1. Os profissionais alocados pela **CONTRATADA** nas atividades deverão possuir capacitação mínima para o exercício das atividades nos ambientes do TJCE, o que contempla:

4.15.1.1. Formação técnica ou superior em Tecnologia da Informação, Redes de Computadores, Segurança da Informação ou áreas correlatas;

4.15.1.2. Experiência comprovada em implantação, operação e suporte de soluções de balanceamento de carga (ADC) e/ou Web Application Firewall (WAF), conforme o lote de atuação;

4.15.2. Especificamente para as atividades de instalação, configuração e suporte da solução contratada, deverá haver comprovação de qualificação em certificações técnicas do fabricante da solução ofertada (ex.: F5, Fortinet, Citrix ou equivalente), em boas práticas de segurança da informação (ex.: ISO/IEC 27001, OWASP) ou certificação equivalente, desde que devidamente comprovada a capacidade técnica compatível com a solução ofertada.

4.15.3. Para a execução das atividades relacionadas ao WAF como Serviço (SaaS), a CONTRATADA deverá comprovar que os profissionais alocados possuem experiência comprovada na implantação e operação de soluções WAF em ambiente de nuvem, com certificações relevantes de segurança e governança em cloud, tais como Cloud Security Professional (CCSP), AWS Certified Security, Microsoft Azure Security Engineer Associate, certificações de segurança da informação como ISO/IEC 27001 ou CompTIA Security+ ou certificação equivalente, desde que devidamente comprovada a capacidade técnica compatível

com a solução ofertada.

4.15.4. Adicionalmente, será exigido que o provedor de nuvem (Cloud Broker) seja certificado em normas de segurança e conformidade reconhecidas internacionalmente, como ISO/IEC 27017 (Segurança na Nuvem), ISO/IEC 27018 (Proteção de Dados Pessoais na Nuvem) e SOC 2 Tipo II, garantindo aderência às melhores práticas de proteção e privacidade de dados.

4.16. **Requisitos de formação da equipe**

4.16.1. Os serviços deverão ser prestados por técnicos devidamente capacitados, de acordo com os critérios estabelecidos a seguir:

4.16.2. Os profissionais técnicos deverão possuir formação técnica ou superior em Tecnologia da Informação, Redes de Computadores, Segurança da Informação ou áreas correlatas, além das certificações específicas exigidas para cada lote, conforme os requisitos de qualificação profissional;

4.16.3. Será designado um Gerente de Projetos, responsável pela coordenação de todas as atividades de migração, instalação, configuração e homologação das soluções, devendo comprovar experiência mínima de 2 (dois) anos em gestão de projetos de TI e possuir certificação reconhecida como PMP (Project Management Professional), PRINCE2 ou certificação equivalente, desde que devidamente comprovada a capacidade técnica compatível com a solução ofertada.

4.17. **Requisitos de metodologia**

4.17.1. O fornecimento dos equipamentos está condicionado ao recebimento pelo Contratado de Ordem de Fornecimento (OF) ou Ordem de Serviços (OS) emitida pela Contratante.

4.17.2. A OF/OS indicará o tipo de equipamento/serviços, a quantidade e a localidade na qual as soluções deverão ser entregues.

4.17.3. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma:

4.17.4. Atendimento eletrônico e telefônico disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

4.17.5. O andamento do fornecimento dos equipamentos e da prestação dos serviços deverá ser acompanhado pelo Contratado, que dará ciência de eventuais ocorrências à Contratante, por meio de relatórios eletrônicos periódicos e comunicações formais.

4.17.6. O Contratado deverá adotar metodologia de gestão de projetos baseada em boas práticas reconhecidas (ex.: PMBOK, PRINCE2 ou equivalente), contemplando planejamento, execução, monitoramento e controle das atividades, bem como gerenciamento de riscos, garantindo que todas as etapas sejam executadas dentro dos prazos, custos e qualidade estabelecidos no contrato.

4.17.7. O Contratado deverá disponibilizar um Service Desk estruturado conforme as melhores práticas do ITIL, com registro e acompanhamento de chamados, categorização por níveis de prioridade (P1 a P4), escalonamento de incidentes, emissão de relatórios periódicos e integração com a equipe técnica do TJCE para solução e tratamento de incidentes dentro dos prazos estabelecidos nos Acordos de Nível de Serviço (SLA)

4.18. **Requisitos de segurança da informação e privacidade**

4.18.1. A **CONTRATADA** deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

4.18.2. Não poderá:

4.18.3. Utilizar os dados, sistemas ou informações do TJCE para fins distintos da execução contratual;

4.18.4. Armazenar, transferir ou processar informações do TJCE em ambientes ou serviços não autorizados e não conformes com os requisitos de segurança estabelecidos;

4.18.5. Permitir acesso de terceiros não autorizados às informações, sistemas e aplicações do TJCE;

4.18.6. Realizar cópias, extrações ou transferências de dados sem autorização formal da Contratante.

4.18.7. Compartilhar informações com subcontratadas/processadoras sem anuência prévia e formal do TJCE, inclusive quanto às cláusulas de proteção de dados.

4.18.8. Deverá:

4.18.9. Cumprir integralmente as diretrizes da Política de Segurança da Informação (PSI) do TJCE (Resolução do Órgão Especial nº 15/2023), as normas do CNJ, a LGPD (Lei nº 13.709/2018) e demais regulamentos aplicáveis;

4.18.10. Adotar criptografia para dados em trânsito (p.ex., TLS 1.2+ ou superior) e em repouso, quando aplicável, com gestão de chaves adequada;

4.18.11. Garantir autenticação e controle de acesso (princípio do menor privilégio, segregação de funções e, quando aplicável, MFA) para todos os perfis de usuário e administrador da solução;

4.18.12. Registrar e manter trilhas de auditoria e logs de operações, incidentes e acessos relacionados à solução, com retenção e proteção dos registros pelo prazo e forma definidos na PSI; integrar os logs ao SIEM do TJCE, quando aplicável;

4.18.13. Implementar medidas técnicas e organizacionais de proteção (endurecimento, correções, gestão de vulnerabilidades, varreduras/perfis periódicos), mantendo evidências de execução;

4.18.14. Disponibilizar relatórios periódicos de segurança e notificar a Contratante imediatamente em caso de incidentes que afetem a confidencialidade, integridade ou disponibilidade das informações.

4.18.15. Definir, documentar e seguir procedimentos de backup e restauração dos registros/artefatos sob sua guarda, com testes periódicos e níveis de serviço compatíveis com os requisitos do contrato.

4.18.16. Assegurar documentação atualizada da arquitetura física e lógica da solução, dos controles implementados e dos pontos de integração; disponibilizar ao TJCE sempre que solicitado.

4.18.17. Apoiar, quando aplicável, a realização de Análise de Risco e Relatório de Impacto à Proteção de Dados (RIPD/DPIA) relativos ao tratamento de dados pessoais no escopo da solução.

4.18.18. Estabelecer cláusulas contratuais com eventuais operadoras/subprocessadoras contemplando obrigações de segurança e privacidade equivalentes às exigidas pelo TJCE, inclusive quanto à localização/transferência internacional de dados, quando aplicável

4.19. **Outros requisitos aplicáveis**

4.19.1. **Requisitos de sustentabilidade**

4.19.1.1. Além dos parâmetros específicos de sustentabilidade intrinsecamente vinculados ao tipo de objeto contratual, a **CONTRATADA** deve estar em conformidade com exigências que

fomentem a adoção de boas práticas destinadas a otimizar o uso de recursos, reduzir a incidência de desperdícios, mitigar a poluição e considerar atentamente as preocupações de cunho social.

4.19.1.2. Estes critérios englobam:

4.19.1.2.1. Racionalização do uso de substâncias potencialmente tóxicas ou poluentes, visando à proteção da saúde e do meio ambiente.

4.19.1.2.2. Adoção de embalagens sustentáveis e de baixo impacto ambiental, priorizando materiais recicláveis, reutilizáveis ou biodegradáveis. A **CONTRATADA** deve buscar minimizar o desperdício de recursos na embalagem de seus produtos, bem como considerar opções que reduzam a geração de resíduos sólidos e contribuam para a preservação do meio ambiente. Além disso, a embalagem deve ser projetada de forma eficiente, levando em consideração seu transporte e armazenamento, com o objetivo de reduzir as emissões de carbono associadas à logística.

4.19.1.2.3. Substituição de substâncias tóxicas por alternativas atóxicas ou de menor toxicidade, garantindo a segurança dos trabalhadores e a preservação ambiental.

4.19.1.2.4. Adoção de práticas que promovam a racionalização e economia no consumo de energia elétrica e água, contribuindo para a redução dos impactos ambientais.

4.19.1.2.5. Treinamento e capacitação periódicos dos empregados, com foco em boas práticas de redução de desperdícios, poluição e considerações sociais, visando ao desenvolvimento sustentável.

4.19.1.2.6. Implementação de programas de reciclagem e destinação adequada dos resíduos gerados nas atividades de limpeza, asseio e conservação, reduzindo o impacto ambiental e fomentando a inclusão social.

4.19.1.2.7. Promoção da utilização de água de reuso ou outras fontes, como águas pluviais ou de poços certificados como isentos de contaminação por metais pesados ou agentes bacteriológicos, sempre que viável, visando a conservação dos recursos hídricos e a preocupação social com o acesso à água limpa.

4.19.1.3. Dessa forma, a **CONTRATADA** não apenas se compromete com a sustentabilidade ambiental, mas também com o bem-estar da sociedade, cumprindo requisitos que abrangem tanto aspectos ecológicos quanto sociais.

5. RESPONSABILIDADES

5.1. **Deveres e responsabilidades do TJCE**

5.1.1. O TJCE deverá cumprir todas as obrigações constantes no Edital e seus anexos e ainda:

5.1.1.1. Prestar à **CONTRATADA**, em tempo hábil, as informações eventualmente necessárias ao fornecimento respectivo;

5.1.1.2. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

5.1.1.3. Viabilizar local para entrega, teste ou instalação, o que couber segundo o tipo de objeto.

5.1.1.4. Efetuar os pagamentos nos valores e prazos dispostos neste instrumento;

5.1.1.5. Acompanhar os relatórios de consumo disponibilizados, devendo notificar à CONTRATADA qualquer anormalidade constatada;

5.1.1.6. Analisar Relatório Mensal de Consumo, encaminhado pela CONTRATADA, em até 15 dias após o seu recebimento;

5.1.1.7. Caso sejam apuradas divergências contidas no Relatório, o TJCE deverá comunicar imediatamente à contratada. Se não o fizer no prazo estabelecido acima, a CONTRATADA entenderá como aceite do relatório.

5.1.1.8. Utilizar os serviços contratados em rígida observância às legislações e às regulamentações em vigor no âmbito municipal, estadual e federal, de maneira zelosa, prezando sempre pela segurança, pela estabilidade e pela confiabilidade dos serviços e ambientes técnicos;

5.1.1.9. Não utilizar aplicação, sistema e/ou funcionalidade, objeto deste contrato, para promover, intermediar, divulgar facilitar ou incentivar ações ilegais, ilícitas ou irregulares, ficando o TJCE integral e exclusivamente responsável nas esferas civil e penal na eventual ocorrência desses fatos;

5.1.1.10. Responsabilizar-se, exclusivamente, por toda e qualquer aplicação, sistema, serviço, configuração ou funcionalidade, por ela desenvolvida ou por terceiros, que esteja sendo executada em conjunto com o serviço da CONTRATADA; bem como por toda e qualquer ação de sua parte, seja ela proposital ou não, quando da utilização dos serviços contratados;

5.1.1.11. Comunicar de imediato, por meio dos canais oficiais de suporte, toda e qualquer descoberta de vulnerabilidade de segurança em seus sistemas, aplicações ou funcionalidades que possa comprometer a estabilidade do ambiente técnico ou o funcionamento dos serviços, ficando responsável, também, por corrigir tais vulnerabilidades e comunicar a correção à CONTRATADA;

5.1.1.12. Retirar as aplicações do ambiente de nuvem da CONTRATADA ao término da vigência do contrato ou nas hipóteses de rescisão contratual;

5.1.1.13. Prestar, por meio de seu gestor do contrato, as informações e os esclarecimentos pertinentes ao serviço contratado que venham a ser solicitados pela CONTRATADA;

5.1.1.14. Registrar os incidentes e problemas ocorridos durante a execução do contrato;

5.1.1.15. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução do contrato;

5.1.1.16. Encaminhar formalmente a demanda, por meio de Ordem de Serviço, de acordo com os critérios estabelecidos em Contrato;

5.1.1.17. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita;

5.1.1.18. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis;

5.1.1.19. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em Contrato;

5.1.1.20. Informar à CONTRATADA sobre atos que possam interferir direta ou indiretamente nos fornecimentos e serviços prestados;

5.1.1.21. Proporcionar os recursos técnicos e logísticos necessários para que a CONTRATADA possa realizar os fornecimentos e executar os serviços conforme as especificações estabelecidas em Contrato;

5.1.1.22. Comunicar oficialmente à CONTRATADA sobre quaisquer falhas verificadas na fiscalização do cumprimento dos fornecimentos e serviços prestados;

5.1.1.23. Revogar e eliminar autorizações de acesso e caixas postais concedidas à CONTRATADA e a seus representantes ao final do contrato e quando houver substituições na equipe que atende ao TJCE; e

5.1.1.24. Disponibilizar cópia da Política de Segurança da Informação (PSI/TJCE) e das demais normas pertinentes à execução dos serviços, bem como as suas atualizações.

5.1.1.25. As responsabilidades atribuídas à CONTRATANTE não afastam a responsabilidade da CONTRATADA quanto à qualidade, segurança, desempenho e adequada prestação da solução contratada.

5.2. **Deveres e responsabilidades da contratada**

5.2.1. A **CONTRATADA** deverá cumprir todas as obrigações constantes no Edital, seus anexos e na sua proposta, assumindo os seus riscos e as despesas decorrentes da boa e perfeita execução do objeto.

5.2.2. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste Termo de Referência, acompanhado da respectiva nota fiscal, na qual constarão ao menos as indicações referentes a: número de empenho, número do processo, marca, fabricante, modelo, procedência e prazo de garantia ou validade;

5.2.3. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), reconhecendo desde já a aplicabilidade desta legislação específica no fornecimento detalhado neste instrumento;

5.2.4. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

5.2.5. Comunicar ao TJCE, no prazo máximo de 48 (quarenta e oito) horas que antecede a data da execução ou entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

5.2.6. Garantir que o insumo fornecido será recolhido e substituído, sem ônus para o TJCE, caso ele não esteja de acordo com os padrões de qualidade exigidos;

5.2.7. Efetuar a troca do produto, caso ele deteriore, mesmo em condições ambientais adequadas de estocagem;

5.2.8. Cumprir o contrato dentro do prazo estipulado, em conformidade com as especificações constantes neste Termo de Referência e na quantidade solicitada;

5.2.9. Assumir todas as responsabilidades e custos decorrentes de encargos trabalhistas, previdenciários, fiscais, comerciais, de transporte, seguros e demais tributos incidentes sobre a execução do contrato.;

5.2.10. Atender prontamente o representante do TJCE com vista às substituições dos materiais que tenham sido recusados pela Administração;

5.2.11. Manter à frente pessoa qualificada, para representá-lo junto à fiscalização do TJCE;

5.2.12. Fornecer os materiais nas embalagens originais e adotar todas as medidas preventivas no sentido de se minimizar acidentes ou danos que venham a comprometer a qualidade e a quantidade fornecida;

5.2.13. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, e responder por danos causados diretamente a terceiros ou ao TJCE, independentemente da comprovação de sua culpa ou dolo na execução do contrato;

5.2.14. Responsabilizar-se por quaisquer ônus, despesas, obrigações trabalhistas, previdenciárias, fiscais, de acidentes de trabalho, bem como alimentação, transporte ou outro benefício de qualquer natureza e com todos os encargos sociais previstos na legislação vigente e de quaisquer outros em decorrência da sua condição de empregadora.

5.2.15. Prestar os Serviços de forma alinhada aos termos especificados neste Termo de Referência, dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica, normas e legislação, mantendo a qualidade dos serviços prestados, de maneira uniforme, durante toda a vigência do presente documento jurídico;

5.2.16. Executar o objeto em conformidade com as condições deste instrumento;

5.2.17. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

5.2.18. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitados ao estabelecido na Lei Federal nº 14.133/2021, tomando-se por base o valor contratual;

5.2.19. Responsabilizar-se pelos danos causados diretamente ao TJCE ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual;

5.2.20. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas;

5.2.21. Refazer o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações deste termo, no prazo de 5 (cinco) dias, contados da sua notificação;

5.2.22. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta, observando o prazo mínimo exigido pela Administração;

5.2.23. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização da contratante;

5.2.24. Encaminhar ao TJCE, até o 5º (quinto) dia útil do mês seguinte ao da prestação dos serviços, o Relatório de nível de serviço;

5.2.25. Considera-se mês de prestação dos serviços o período compreendido entre o primeiro e último dia do mês, podendo este ser proporcional no mês de início e de término da vigência contratual ou no caso de suspensão/interrupção contratual.

5.2.26. Aplicar ajustes nos relatórios, caso as contestações do TJCE tenham fundamento;

5.2.27. Disponibilizar ao TJCE os relatórios de consumo dos serviços contratados a qualquer tempo, via solicitação ou sistema;

5.2.28. Remeter a Nota Fiscal ou Fatura e Documento de Arrecadação Estadual – DAE via correio eletrônico, para endereço eletrônico indicado pelo TJCE;

5.2.29. Prestar suporte técnico e fornecer um canal oficial especializado para atender demandas operacionais da TJCE, sempre de acordo com os processos de atendimento definidos por este Termo de Referência;

5.2.30. Comunicar ao TJCE qualquer alteração nos canais de suporte técnico e nos seus respectivos processos de atendimento e tramitação de suporte. As alterações não entrarão em vigor sem que ocorra a notificação ao TJCE;

5.2.31. Uma vez realizada a notificação ao TJCE acerca das modificações acima mencionadas, após a confirmação de ciência do TJCE, tais alterações poderão ser aplicadas de maneira imediata.

5.2.32. Comunicar ao TJCE, com antecedência mínima de 48 (quarenta e oito) horas, a necessidade de interrupção ou degradação do serviço por motivo de manutenção, atualização ou qualquer outro evento que possa, de alguma forma, interferir na prestação dos serviços que são objeto deste Termo de Referência;

5.2.33. Tornar disponíveis ao TJCE informações sobre características e especificações técnicas necessárias à prestação do serviço;

5.2.34. Prestar esclarecimentos ao TJCE sobre eventuais atos ou fatos noticiados que envolvam a prestação de serviços independente de solicitação;

5.2.35. Zelar pela segurança e confidencialidade das informações que tiver acesso;

5.2.36. Garantir que todas as informações do TJCE estarão armazenadas em ambientes técnicos (datacenters) localizados dentro dos limites do território brasileiro;

5.2.37. Promover, em caso de desastres nas estruturas técnicas, manobras entre datacenters, em regime emergencial, para manutenção da alta disponibilidade dos serviços;

5.2.38. Reportar formal e imediatamente ao Gestor do Contrato quaisquer problemas, anormalidades, indisponibilidades, erros e irregularidades que possam comprometer a execução do serviço, considerando que:

5.2.39. Episódios de indisponibilidade serão caracterizados pelo não funcionamento de um serviço em situações não previstas ou planejadas;

5.2.40. Paralisações nos serviços que forem executadas de maneira planejada, sejam elas parciais ou totais, de natureza corretiva ou evolutiva, não serão caracterizadas como indisponibilidade; e

5.2.41. Indisponibilidades, totais ou parciais, ocasionadas por eventos de caso fortuito ou força maior, não poderão ser computadas para cálculo do SLA.

5.2.42. Seguir as instruções e observações efetuadas pelo Gestor do Contrato, e/ou fiscais técnicos;

5.2.43. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do TJCE, referentes a qualquer problema detectado ou ao andamento de atividades previstas;

5.2.44. Detalhar e repassar, conforme orientação e interesse do TJCE, o conhecimento técnico utilizado na execução do serviço contratado.

5.2.45. Indicar PREPOSTO e cuidar para que este mantenha permanente contato com o Gestor do Contrato e adote as providências requeridas, além de comandar, coordenar e controlar a execução do serviço contratado, inclusive a gestão dos seus profissionais;

5.2.46. Recrutar e selecionar os profissionais necessários à realização do serviço, de acordo com a

qualificação técnica adequada;

5.2.47. Providenciar e manter qualificação técnica adequada dos profissionais que prestam serviço para o TJCE;

5.2.48. Planejar, desenvolver, implantar, executar e manter o objeto do contrato dentro dos níveis de serviço exigidos e dos indicadores;

5.2.49. Responsabilizar-se integralmente por sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante a vigência do Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas, caso os prazos, níveis, indicadores e condições não sejam cumpridos;

5.2.50. Elaborar e apresentar, mensalmente, Relatório Gerencial das Ordens de Serviços executadas, contendo detalhamento dos níveis de serviço executados em confronto aos exigidos, as eventuais justificativas no caso de desempenho inferior ao padrão esperado e demais informações necessárias ao acompanhamento e avaliação da execução do serviço;

5.2.51. Elaborar e apresentar, mensalmente, Relatório Detalhado de Utilização dos Serviços, devendo o relatório ser gerado a partir de fonte primária de administração dos serviços;

5.2.52. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do objeto do Contrato, respeitando todos os critérios de sigilo, segurança e inviolabilidade, e aplicáveis aos dados, informações, regras de negócios, documentos, entre outros;

5.2.53. Cumprir e garantir que seus profissionais estejam cientes do Termo de Confidencialidade da Informação, das normas e dos procedimentos estabelecidos na Política de Segurança da Informação do TJCE.

5.2.54. Entender como mínimas todas as características técnicas apresentadas neste Termo de Referência, sendo aceitas características e desempenhos superiores ao solicitado;

5.2.55. A CONTRATADA é responsável, exclusiva e direta, por todos os contratados utilizados na operação dos serviços e no cumprimento das obrigações previstas neste Termo de Referência.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. **Rotinas de execução**

6.1.1. A execução do contrato será acompanhada por representante(s) do TJCE, definido(s) como Gestor e Fiscal(is) do Contrato, que manterá(ão) comunicação com o representante indicado pela **CONTRATADA**, denominado PREPOSTO.

6.1.2. A **CONTRATADA** designará formalmente o PREPOSTO da **CONTRATADA**, na forma do modelo do Anexo III, que deverá manter-se acessível e disponível para tratamento das questões executivas do contrato por todo o período de realizações contratuais, podendo a **CONTRATADA** nomear mais de um PREPOSTO para o encargo, quando necessário.

6.1.3. As comunicações entre o TJCE e a **CONTRATADA** devem ser realizadas por escrito, preferencialmente por meio eletrônico, em sistema oficial de protocolo ou ferramenta formalmente aprovada, e concentradamente pelo representante legal da **CONTRATADA** ou preposto do contrato.

6.1.4. A fiscalização poderá ser efetivada por amostragem e com base em critérios estatísticos, levando-se em consideração falhas que impactem o contrato como um todo, os níveis de serviço (SLA) e os indicadores de desempenho estabelecidos.

6.1.5. A fiscalização da execução será efetuada pelo fiscal técnico, que acompanhará o cumprimento e exigirá que sejam cumpridas todas as exigências relacionadas ao fornecimento, de modo a assegurar os melhores resultados para o TJCE.

6.1.6. A fiscalização técnica deve avaliar, através do Instrumento de Medição de Resultado (IMR), a qualidade e condições da entrega e recebimento dos objetos, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos.

6.1.7. A fiscalização técnica deve monitorar a qualidade dos objetos entregues em cotejo com as especificações deste Termo de Referência, devendo intervir para requerer à **CONTRATADA** a correção das faltas, falhas e irregularidades constatadas.

6.1.8. Poderão ser exigidos documentos comprobatórios e evidências da **CONTRATADA**, para confrontar com a proposta e detalhamentos deste Termo de Referência em busca da conferência de adequação.

6.1.9. A fiscalização abrange, ainda, as seguintes verificações específicas nos serviços prestados:

6.1.9.1. Cumprimento dos prazos, níveis de serviço (SLA) e indicadores de desempenho definidos neste Termo de Referência;

6.1.9.2. Atendimento integral aos requisitos de segurança da informação, confidencialidade e integridade dos dados, conforme a Política de Segurança da Informação do TJCE.

6.1.10. A fiscalização não exclui nem reduz a responsabilidade da **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios ou não, emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do TJCE ou de seus agentes.

6.1.10.1. Tratando-se de equipamentos, materiais, insumos ou quaisquer outros alcances fornecidos pelo TJCE para a realização das atividades, deverá a **CONTRATADA** avaliar a adequação dos mesmos e solicitar substituição, quando inadequados, não sendo admitido associar a falta de qualidade destes ao resultado dos serviços, vez que o conhecimento técnico mais apurado e responsabilidade pelas entregas finais de serviços são da **CONTRATADA**.

6.1.11. A fiscalização do TJCE anotará no histórico do contrato todas as ocorrências relacionadas à sua execução, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados, podendo exigir da **CONTRATADA** acompanhamento e participação nos registros e restando a **CONTRATADA** obrigada a cumprir a exigência.

6.1.12. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção, sem prejuízo de promover o sancionamento porventura cabível.

6.2. **Quantidade mínima de bens ou serviços para comparação e controle**

6.2.1. Cada OF/OS conterá a quantidade a ser fornecida, incluindo a sua localização e o prazo, conforme definições deste TR.

6.3. **Mecanismos formais de comunicação**

6.3.1. São definidos como mecanismos formais de Comunicação, entre a Contratante e o Contratado, os seguintes:

6.3.1.1. Ordem de Fornecimento (OF);

6.3.1.2. Ordem de Serviços (OS);

6.3.1.3. Ata de Reunião;

6.3.1.4. Ofício;

6.3.1.5. Sistema de abertura e acompanhamento de chamados técnicos e administrativos;

6.3.1.6. E-mails e cartas formais, preferencialmente por meio de endereços institucionais previamente autorizados;

6.3.1.7. Relatórios técnicos e gerenciais, conforme modelos definidos neste Termo de Referência;

6.3.1.8. Comunicados eletrônicos via sistemas oficiais do TJCE, quando aplicável;

6.3.1.9. Protocolos e notificações formais emitidos pela fiscalização do contrato;

6.3.1.10. Reuniões técnicas presenciais ou remotas, previamente convocadas e registradas em ata.

6.4. **Manutenção de sigilo e normas de segurança**

6.4.1. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução do contrato, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.4.2. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos ANEXOS IV e V.

6.4.3. O Contratado deverá observar integralmente a Política de Segurança da Informação (PSI) do TJCE, definida pela Resolução do Órgão Especial nº 15/2023, bem como as normas do Conselho Nacional de Justiça (CNJ) aplicáveis à segurança cibernética e à Lei Geral de Proteção de Dados (Lei nº 13.709/2018), adotando medidas técnicas e administrativas para garantir a confidencialidade, integridade e disponibilidade das informações.

6.4.4. Qualquer incidente de segurança que comprometa dados, sistemas ou informações deverá ser comunicado imediatamente ao TJCE, por meio dos canais oficiais, com fornecimento de todas as informações necessárias para a análise, mitigação e correção do incidente.

6.5. **Formas de transferência de conhecimento**

6.5.1. A transferência do conhecimento deverá ser realizada observando-se o que segue:

6.5.1.1. A CONTRATADA deverá realizar a transferência de conhecimento por meio dos treinamentos técnicos e funcionais previstos neste Termo de Referência, abrangendo a instalação, configuração, operação, manutenção e segurança das soluções implantadas;

6.5.1.2. A transferência deverá incluir a entrega de documentação técnica detalhada, manuais de operação, relatórios de configuração e a realização de sessões formais de esclarecimentos, garantindo que o TJCE tenha condições de operar e manter as soluções de forma autônoma ao término da implantação.

6.6. **Procedimentos de transição e finalização do contrato**

6.6.1. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:

6.6.1.1. A CONTRATADA deverá elaborar e executar um Plano de Transição, com transferência de tecnologia e técnicas empregadas, sem perda de informações, aos técnicos do TJCE ou do fornecedor de uma nova Solução de Tecnologia da Informação adquirida ao final da vigência da presente contratação.

6.6.1.2. O Plano de Transição deverá ser apresentado pela CONTRATADA 90 (noventa) dias antes do encerramento do contrato para aprovação do TJCE.

6.6.1.3. Planejamento da transição, elaborado pela CONTRATADA em conjunto com o TJCE, contendo cronograma, atividades, responsáveis, riscos e plano de contingência, garantindo a continuidade dos serviços até a finalização contratual;

6.6.1.4. Transferência de conhecimento, por meio de treinamentos, documentação técnica, relatórios de configuração e manuais de operação, assegurando que a equipe técnica do TJCE detenha toda a informação necessária para a manutenção, operação e evolução da solução após o término contratual;

6.6.1.5. Entrega formal dos ativos, documentação final, credenciais e configurações ao TJCE, assegurando a integridade e segurança das informações e sistemas;

6.6.1.6. Revogação de acessos, com a exclusão de todos os perfis e credenciais da CONTRATADA em sistemas, redes e ambientes do TJCE, bem como a devolução de eventuais equipamentos e mídias utilizadas durante a execução contratual;

6.6.1.7. Relatório de encerramento, elaborado pela CONTRATADA e validado pelo TJCE, detalhando todas as atividades executadas, pendências resolvidas, níveis de serviço atingidos e indicadores de desempenho finais.

6.6.1.8. É vedada qualquer retenção de informações, configurações ou dependência tecnológica que impeça a plena transferência de conhecimento à CONTRATANTE ou a terceiros por ela indicados.

7. MODELO DE GESTÃO DO CONTRATO

7.1. Após a entrega e/ou disponibilização da solução, conforme o lote contratado, o TJCE iniciará o processo de verificação e aceitação do objeto, com vistas à emissão dos Termos de Recebimento Provisório (TRP) e Definitivo (TRD), nos termos do art. 140 da Lei nº 14.133/2021. O recebimento provisório não implica aceitação definitiva nem prejudica a apuração de vícios, desconformidades ou ajustes técnicos que possam ser identificados posteriormente.

7.2. O recebimento do objeto seguirá a seguinte dinâmica:

7.2.1. Concluída a entrega dos equipamentos, implantação da solução, configuração inicial e/ou disponibilização dos serviços ou produtos, a CONTRATADA deverá comunicar formalmente ao TJCE a conclusão da etapa de implantação, conforme prazos estabelecidos no item 4.6.10, apresentando relatório técnico de implantação contendo evidências do atendimento aos requisitos previstos neste Termo de Referência.

7.2.2. Para o Lote 1 – Solução ADC (aquisição de bens e licenciamento) - Relatório de implantação deverá comprovar, no mínimo:

7.2.2.1. Entrega física dos equipamentos conforme especificação contratual;

7.2.2.2. Instalação e energização dos equipamentos;

7.2.2.3. Configuração inicial e integração com o ambiente do TJCE;

7.2.2.4. Execução dos testes de funcionamento, alta disponibilidade e balanceamento de

carga;

7.2.2.5. Ativação e validação das licenças perpétuas;

7.2.2.6. Funcionamento pleno da solução em ambiente operacional;

7.2.2.7. Validação dos testes de desempenho e alta disponibilidade;

7.2.2.8. Entrega da documentação técnica preliminar da solução;

7.2.2.9. Entrega e aprovação da documentação técnica definitiva em conformidade com as especificações técnicas presentes no ANEXO I – ESPECIFICAÇÕES TÉCNICAS – LOTE 1;

7.2.2.10. Ausência de pendências técnicas impeditiva do funcionamento do ADC na rede interna.

7.2.3. Para o Lote 2 – Solução WAF (SaaS) - Relatório de implantação deverá comprovar, no mínimo:

7.2.3.1. Disponibilização da solução em ambiente produtivo;

7.2.3.2. Configuração inicial das políticas de segurança;

7.2.3.3. Integração com os sistemas e aplicações do TJCE;

7.2.3.4. Ativação dos mecanismos de proteção (WAF, anti-DDoS, API, etc.);

7.2.3.5. Validação inicial de funcionamento e acesso;

7.2.3.6. Solução em pleno funcionamento em ambiente produtivo;

7.2.3.7. Validação das políticas de segurança e proteção implementadas;

7.2.3.8. Entrega da documentação técnica preliminar da solução em conformidade com as especificações técnicas presentes no ANEXO II – ESPECIFICAÇÕES TÉCNICAS – LOTE 2;

7.2.3.9. Ausência de pendências técnicas impeditiva do funcionamento das aplicações publicadas do TJCE.

7.2.4. Será verificada, no que couber, a manutenção da idoneidade trabalhista e previdenciária.

7.2.5. Após a entrega do relatório de implantação, o TJCE emitirá o Termo de Recebimento Provisório (TRP), iniciando-se o prazo de até 5 (cinco) dias úteis para validação da implantação, conforme estabelecido no art. 140 da Lei nº 14.133/2021.

7.2.6. Caso sejam identificadas pendências ou inconformidades, a CONTRATADA será formalmente notificada para correção. Havendo pendências:

7.2.6.1. A CONTRATADA deverá realizar as correções no prazo de até 15 (quinze) dias corridos, contados da notificação;

7.2.6.2. Após a correção, será reiniciado o processo de validação do recebimento provisório.

7.2.7. Após a validação sem pendências da implantação, será assinado o Termo de Recebimento Definitivo (TRD) de implantação, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021.

7.2.7.1. A inicialização dos serviços (item 2 do Lote 1 e itens 1 e 3 do Lote 2) será considerada inicializada somente após a emissão do TRD por parte do TJCE para finalidade de pagamento.

7.2.7.2. Conforme descrito no ANEXO II – ESPECIFICAÇÕES TÉCNICAS – LOTE 2, o consumo do quantitativo do item 2 do Lote 2 será sob demanda via emissão de Ordem de Serviço de acordo com a necessidade do TJCE.

7.2.8. O recebimento e aceitação dos serviços, inclusive quando conte com subcontratação, não excluirá a responsabilidade civil da CONTRATADA pela qualidade, durabilidade, solidez e pela segurança do serviço, nem a responsabilidade ético-profissional pela perfeita execução do contrato.

8. CRITÉRIOS DE MEDIÇÃO

8.1. **Níveis mínimos de serviço exigidos**

8.1.1. O preço fixado em contrato para a prestação dos serviços se referirá à execução com a máxima qualidade. Portanto, a execução contratual que atenda, mesmo que parcialmente, os objetivos contratados sem a máxima qualidade, importará pagamento proporcional pelo realizado, seguindo os critérios definidos neste instrumento e constantes dos anexos.

8.1.2. Tais ajustes visam assegurar o recebimento dos objetos, mesmo diante de eventuais imperfeições em sua execução, com a dedução prevista no artigo 144 da Lei nº 14.133/21, promovendo-se pagamento proporcional ao realizado, de modo a evitar superfaturamento e locupletamento.

8.1.3. Entretanto, eventuais falhas e descumprimentos contratuais verificados, seja por não estarem nas previsões ou faixas de admissibilidade dos instrumentos de medição de resultados, seja por se situarem no nível mínimo destas, serão devidamente apurados em processos administrativos próprios, podendo resultar em aplicação de penalidade, sem prejuízo de possível rescisão do contrato.

8.1.4. Após terminado o mês de prestação dos serviços, o representante do TJCE apresentará à **CONTRATADA** o instrumento "Medição de Serviços Prestados" que conterá, no mínimo:

8.1.4.1. Número do processo administrativo de contratação que deu origem ao contrato;

8.1.4.2. Número do Contrato;

8.1.4.3. Partes Contratuais;

8.1.4.4. Síntese do objeto;

8.1.4.5. Listagem de ocorrências e medições;

8.1.4.6. Fator percentual de aceitação e remuneração dos serviços.

8.1.5. A **CONTRATADA** deve avaliar com atenção os impactos prováveis do instrumento "Medição de Serviços Prestados" ante a qualidade esperada dos seus serviços e respectivos impactos financeiros, de modo a precificar com responsabilidade, pois não haverá flexibilização de medições ou de valores a serem pagos.

8.2. **Instrumento de Medição de Resultados (IMR)**

8.2.1. A avaliação do desempenho do suporte técnico observará os indicadores e critérios definidos

no Instrumento de Medição de Resultado – IMR, constante no ANEXO VI deste Termo de Referência.

8.3. **Sanções administrativas**

8.3.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

8.3.1.1. der causa à inexecução parcial do contrato;

8.3.1.2. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

8.3.1.3. der causa à inexecução total do contrato;

8.3.1.4. ensejar o retardamento da execução ou da entrega do objeto da contratação sem

8.3.1.5. motivo justificado;

8.3.1.6. apresentar documentação falsa ou prestar declaração falsa durante a execução

8.3.1.7. do contrato;

8.3.1.8. praticar ato fraudulento na execução do contrato;

8.3.1.9. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

8.3.1.10. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

8.3.2. Com fundamento nos artigos 155 e 156 da Lei nº 14.133/2021, a CONTRATADA estará sujeita às seguintes sanções, conforme tipificação descrita no quadro abaixo:

Tipo de Sanção	Hipóteses de Aplicação
Advertência	Será aplicada quando a CONTRATADA: der causa à inexecução parcial do contrato, quando não se justificar a imposição de penalidade mais grave.
Multa	Será aplicada quando a CONTRATADA: em decorrência de atraso injustificado na execução das obrigações contratuais, descumprimento de níveis de serviço ou inexecução parcial ou total do contrato, observadas as regras de cálculo previstas neste Termo de Referência.
Impedimento de licitar e contratar com o Tribunal de Justiça do Estado do Ceará – TJCE, pelo prazo de até 2 (dois) anos	Poderá ser aplicada quando a CONTRATADA: der causa à inexecução parcial do contrato que cause grave dano à Administração; der causa à inexecução total do contrato; ensejar o retardamento da execução ou da entrega do objeto sem motivo justificado.
Declaração de inidoneidade para licitar ou contratar	Poderá ser aplicada quando a CONTRATADA: apresentar declaração ou documentação falsa; fraudar ou praticar ato fraudulento na execução do contrato; comportar-se de modo inidôneo ou cometer fraude; praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

8.3.3. A multa poderá ser aplicada cumulativamente com as demais sanções administrativas previstas na Lei nº 14.133/2021, em decorrência das infrações previstas no art. 155 da referida lei, observados os critérios de proporcionalidade, gravidade da infração e extensão do dano causado à Administração.

8.3.4. A aplicação e a dosimetria das multas observarão, no que couber, o disposto no Manual de

Aplicação de Penalidades do Tribunal de Justiça do Estado do Ceará – TJCE.

8.3.5. Multa Compensatória

8.3.5.1. A multa compensatória será aplicada nos casos de inexecução parcial ou total do contrato, observados os seguintes percentuais e bases de cálculo:

8.3.5.2. até 10% (dez por cento) sobre o valor do objeto não executado, no caso de inexecução parcial do contrato;

8.3.5.3. até 30% (trinta por cento) sobre o valor global do contrato, no caso de inexecução total do contrato.

8.3.6. Multa de Mora

8.3.6.1. A multa de mora prevista no art. 162 da Lei nº 14.133/2021 será aplicada nos casos de atraso injustificado no cumprimento das obrigações contratuais, incidindo sobre o valor da parcela do fornecimento ou do serviço em mora.

8.3.6.2. A multa de mora será aplicada conforme os seguintes parâmetros:

Fato Gerador (Atraso)	**Alíquota**	**Periodicidade**	**Base de Cálculo**	**Teto (Limite) e Consequência**
Atraso na entrega dos equipamentos necessários à solução, em relação ao prazo contratual	0,5% ao dia até o 30º dia; 0,7% ao dia após o 30º dia	Por dia corrido	valor do item em atraso	Limite de 20%. Atingido o teto, poderá caracterizar inexecução total, a critério da Administração
Atraso na conclusão total do projeto, compreendendo entrega, instalação, configuração, implementação da solução e testes operacionais			valor da parcela do serviço em atraso	Limite de 30%. Atingido o teto, poderá caracterizar inexecução total
Atraso na realização do treinamento			valor total do item	Limite de 5%. Atingido o teto, poderá caracterizar inexecução parcial
Atraso na entrega da documentação técnica (“As Built”)			valor dos itens de instalação	Limite de 20%. Atingido o teto, poderá caracterizar inexecução parcial

8.3.6.3. A CONTRATADA será considerada em atraso também quando entregar os serviços em desconformidade com as especificações técnicas exigidas e não promover a correção ou substituição dentro dos prazos estabelecidos no contrato.

8.3.6.4. A aplicação da multa de mora não impede sua conversão em multa compensatória, nem a

adoção de outras medidas administrativas cabíveis, inclusive a extinção unilateral do contrato quando caracterizada a inexecução parcial ou total.

8.3.7. Penalidades Relacionadas ao IMR

8.3.7.1. A multa de mora também será aplicada, entre outras hipóteses, caso a CONTRATADA não atenda aos prazos e níveis de serviços estabelecidos conforme o Instrumento de Medição de Resultados – IMR, que estabelece os Níveis Mínimos de Serviço – NMS no Anexo VI deste Termo de Referência.

Pontuação IRD (Mês)	Alíquota da Multa	Base de Cálculo
Igual a 3 (três)	1% (um por cento)	Valor total dos itens de suporte/ serviço mensal
Superior a 3 (três)	3% (três por cento)	Valor total dos itens de suporte/ serviço mensal

8.3.7.2. Caso o somatório das multas aplicadas nos 6 (seis) meses anteriores supere 10% (dez por cento) do valor total dos itens de serviço de suporte/ serviço mensal, poderá caracterizar a inexecução parcial ou total do contrato, sem prejuízo da aplicação de outras sanções cabíveis.

8.3.7.3. Em caso de reiterado inadimplemento dos níveis de serviço, a CONTRATANTE poderá aplicar advertência, multa ou outras sanções administrativas previstas neste contrato.

8.3.7.4. Caracterizada a inexecução total do contrato ou a reincidência grave de descumprimento contratual, poderão ser aplicadas as sanções administrativas cabíveis, inclusive a rescisão contratual.

8.3.8. Registro de Ocorrências Operacionais

8.3.8.1. Nos casos de inadimplemento na execução do objeto, as ocorrências poderão ser registradas pela fiscalização contratual, conforme a tabela abaixo:

Id	Ocorrência	Penalidade
1	Não prestar esclarecimentos solicitados pela fiscalização no prazo estabelecido	multa de 0,2% do valor do contrato por dia útil de atraso
2	Descumprimento injustificado de prazos estabelecidos em Ordem de Fornecimento de Bens ou Ordem de Serviço	multa conforme tabela de mora
3	Descumprimento de níveis mínimos de serviço estabelecidos no IMR	aplicação das glosas previstas no IMR
N	Descumprimento de outras obrigações contratuais	advertência ou multa, conforme gravidade

8.3.9. Reincidência de Infrações

8.3.9.1. O reiterado descumprimento das obrigações contratuais ou dos níveis mínimos de serviço

poderá caracterizar inexecução parcial ou total do contrato.

8.3.9.2. Considera-se reincidência, para fins deste Termo de Referência, a repetição da mesma infração por três ou mais ocorrências no período de seis meses.

8.3.9.3. Nessa hipótese, a Administração poderá aplicar penalidade mais gravosa, inclusive multa compensatória ou rescisão contratual, conforme a gravidade da infração.

8.3.10. Caracterização da Inexecução

8.3.10.1. Considera-se inexecução parcial o descumprimento de obrigações contratuais que não inviabilize integralmente a execução do objeto, mas resulte em atraso injustificado, execução defeituosa, reincidência de falhas operacionais ou extrapolação dos limites definidos nos instrumentos de medição de resultados.

8.3.10.2. Considera-se inexecução total a ocorrência de atraso injustificado superior aos prazos máximos estabelecidos, a não entrega do objeto, a paralisação injustificada da execução contratual ou a entrega em desconformidade grave que comprometa definitivamente a finalidade da contratação.

8.3.10.3. A caracterização da inexecução parcial ou total poderá ensejar a rescisão contratual, a aplicação das sanções administrativas cabíveis e a reparação integral dos danos causados à Administração.

8.3.11. Execução das Multas

8.3.11.1. A aplicação de multa de mora não impedirá que a CONTRATANTE a converta em multa compensatória e promova a extinção unilateral do contrato, com a aplicação cumulada das demais sanções previstas neste Termo de Referência e na legislação aplicável.

8.3.11.2. O valor da multa poderá ser descontado das faturas devidas à CONTRATADA.

8.3.11.3. Caso o valor a ser pago à CONTRATADA seja insuficiente para cobrir o valor da multa aplicada, a diferença será descontada da garantia contratual.

8.3.11.4. Se os valores das faturas e das garantias forem insuficientes para a quitação da multa aplicada, a CONTRATADA deverá recolher a importância devida no prazo de 15 (quinze) dias úteis, contados da comunicação oficial.

8.3.11.5. Esgotados os meios administrativos para cobrança do valor devido, o débito poderá ser encaminhado para inscrição em dívida ativa ou para cobrança judicial.

8.3.11.6. Caso o valor da garantia seja utilizado, no todo ou em parte, para pagamento da multa, esta deverá ser recomposta pela CONTRATADA no prazo de 10 (dez) dias úteis, contado da solicitação da CONTRATANTE.

8.3.12. As sanções administrativas observarão o princípio da proporcionalidade e serão aplicadas de forma escalonada, considerando a gravidade da infração, a reincidência e o prejuízo causado à Administração.

8.3.13. A aplicação das sanções será precedida de regular instrução de processo de responsabilização, constituído e conduzido em observância às regras dispostas nos arts. 157 a 161 da Lei n. 14.133/2021 e em regulamento interno da CONTRATANTE, assegurados o contraditório e a ampla defesa.

8.3.14. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade poderão ser aplicadas isoladamente ou cumulativamente com a sanção de multa, nos termos do

art. 156, inciso II e § 7º, da Lei nº 14.133/2021.

8.3.15. A aplicação da sanção de declaração de inidoneidade para licitar ou contratar será precedida de análise jurídica, observadas as regras previstas no § 6º do art. 156 da Lei nº 14.133/2021.

8.3.16. As sanções aplicadas serão registradas no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Portal Nacional de Contratações Públicas (PNCP), conforme previsto no art. 162 da Lei Federal nº 14.133/2021.

8.4. **Do pagamento**

8.4.1. Os pagamentos serão realizados através de depósito bancário preferencialmente nas agências do BANCO BRADESCO S/A, em até 30 (trinta) dias após o recebimento definitivo do objeto constante de cada uma das Ordens de Fornecimento de Bens e/ou Serviços pelo Tribunal de Justiça, mediante apresentação de fatura/nota fiscal, atestada pelo setor competente deste Tribunal de Justiça, e também de apresentação de certidões que comprovem a regularidade da empresa com o fisco Federal, Estadual e Municipal, FGTS e INSS e débitos trabalhistas.

8.4.2. Constatada a situação de irregularidade da CONTRATADA, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do TJCE.

8.4.3. Não havendo regularização ou sendo a defesa considerada improcedente, o TJCE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

8.4.4. Persistindo a irregularidade, o TJCE deverá adotar as medidas necessárias a rescisão do contrato nos autos do processo administrativo correspondente, assegurada a CONTRATADA a ampla defesa.

8.4.5. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação;

8.4.6. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do TJCE, não será rescindido o contrato em execução com a CONTRATADA inadimplente.

8.4.7. Essa(s) nota(s) fiscal(is) /fatura(s) deverá(ão) ser emitida(s) em conformidade com a(s) nota(s) de empenho emitida(s) pelo TJCE.

8.4.8. O Tribunal de Justiça do Ceará não se responsabiliza por qualquer despesa bancária, nem por qualquer outro pagamento não previsto no instrumento contratual;

8.4.9. Havendo erro no documento de cobrança ou outra circunstância que desaprove a liquidação da despesa, a mesma ficará pendente e o pagamento sustado, até que a Contratada providencie as medidas saneadoras necessárias, não ocorrendo, neste caso, quaisquer ônus por parte do Contratante.

8.4.10. Os pagamentos efetuados à CONTRATADA não a isentarão de suas obrigações e responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade do produto.

8.4.11. A CONTRATADA se obriga a manter as condições de habilitação e qualificação exigidas na contratação.

8.4.12. Do pagamento dos serviços sob demanda (Lote 2)

8.4.12.1. O pagamento será devido exclusivamente pelos serviços efetivamente prestados ou consumidos, sendo vedada qualquer cobrança referente à capacidade não utilizada.

8.4.12.2. O pagamento será realizado com base na aferição dos resultados obtidos, conforme os critérios de medição estabelecidos nesta seção e os indicadores definidos no Instrumento de Medição de Resultado (IMR).

8.4.12.3. Para os serviços do Lote 2 (WAF em modelo Software como Serviço – SaaS), o pagamento observará o consumo efetivo de tráfego inspecionado, respeitada a franquia mensal contratada.

8.4.12.4. A franquia adicional de tráfego será utilizada sob demanda, mediante solicitação formal da CONTRATANTE, respeitados os limites máximos estabelecidos no contrato.

8.4.12.5. O consumo será comprovado por meio de relatórios mensais detalhados fornecidos pela CONTRATADA, os quais subsidiarão a medição e o faturamento dos serviços.

8.4.12.6. A utilização da franquia adicional ocorrerá exclusivamente quando houver necessidade operacional devidamente justificada.

9. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

9.1. O custo estimado total da contratação é de R$ 6.804.697,52, conforme detalhamento a seguir e Mapa de Preços constante deste Termo de Referência:

LOTE 1					
Id	**Bem/Serviço**	**UND**	**Qtd.**	**Vlr. Unitário**	**Vlr. Total**
1	Controlador de Entrega de Aplicações (ADC)	**UND**	**2**	**R$ 1.106.223,14**	**R$ 2.212.446,28**
2	Suporte	**MÊS**	**57**	**R$ 12.000,00**	**R$ 684.000,00**
3	Treinamento	**ALUNO**	**8**	**R$ 18.975,00**	**R$ 151.800,00**
4	Instalação	**UND**	**2**	**R$ 65.750,00**	**R$ 131.500,00**
Valor Total - LOTE 1					**R$ 3.179.746,28**

LOTE 2					
Id	**Bem/Serviço**	**UND**	**Qtd.**	**Vlr. Unitário**	**Vlr. Total**
1	Web Application Firewall (WAF) em modelo Software como Serviço (SaaS), com franquia mensal de 50 TB de tráfego inspecionado.	**Mês**	**36**	**R$ 65.291,63**	**R$ 2.350.498,68**
2	Franquia adicional de tráfego inspecionado a ser consumido e contratado sob demanda durante a vigência contratual	**TB**	**900**	**R$ 1.378,21**	**R$ 1.240.389,00**
3	Proteção DNS para 1 zona	**Mês**	**36**	**R$ 946,21**	**R$ 34.063,56**
Valor Total - LOTE 2					**R$ 3.624.951,24**
CUSTO TOTAL ESTIMADO					**R$ 6.804.697,52**

10. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

10.1. A contratação será atendida pela seguinte dotação:

Fonte	Fundo Especial de Modernização do Poder Judiciário do Ceará (FERMOJU)					
Programa	192 - Excelência do Desempenho da Prestação Jurisdicional					
LOTE 01						
ID	**Bem / Serviço**	**QTD**	**Valor Unitário**	**Divisão (1° e 2° Grau)**	**Ação Elemento**	**Valor Total**
1	Controlador de Entrega de Aplicações (ADC)	2	R$ 1.106.223,14	R$ 1.106.223,14	11470 449052	R$ 2.212.446,28
2	Suporte	54	R$ 12.000,00	R$ 648.000,00	11470 449040	R$ 684.000,00
		3		R$ 36.000,00	11473 449040	
3	Treinamento	7	R$ 18.975,00	R$ 132.825,00	20511 339040	R$ 151.800,00
		1		R$ 18.975,00	20512 339040	
4	Instalação	2	R$ 65.750,00	R$ 131.500,00	11470 449040	R$ 131.500,00
Total						**R$ 3.179.746,28**

Fonte	Fundo Especial de Modernização do Poder Judiciário do Ceará (FERMOJU)					
Programa	192 - Excelência do Desempenho da Prestação Jurisdicional					
LOTE 2						
ID	**Serviço**	**QTD**	**Valor Unitário**	**Divisão (1° e 2° Grau)**	**Ação Elemento**	**Valor Total**
1	Web Application Firewall (WAF) em modelo Software como Serviço (SaaS), com franquia mensal de 50 TB de tráfego inspecionado.	34	R$ 65.291,63	R$ 2.219.915,42	11470 449040	R$ 2.350.498,68
		2		R$ 130.583,26	1473 449040	
2	Franquia adicional de tráfego inspecionado a ser consumido e contratado sob demanda durante a vigência contratual	855	R$ 1.378,21	R$ 1.178.369,55	11470 449040	R$ 1.240.389,00
		45		R$ 62.019,45	1473 449040	
3	Proteção DNS para 1 zona	34	R$ 946,21	R$ 32.171,14	11470 449040	R$ 34.063,56
		2		R$ 1.892,42	1473 449040	

			Total		**R$ 3.624.951,24**

10.2. A dotação relativa a compras futuras e exercícios financeiros subsequentes será indicada posteriormente.

11. DA VIGÊNCIA DO CONTRATO

11.1. O prazo original de vigência da contratação pretendida é de 60 (sessenta) meses para o Lote 1 (ADC) e 36 (trinta e seis) meses para o Lote 2 (WAF SaaS), contados a partir da data de assinatura do contrato, sendo permitida a prorrogação, nos termos do art. 107 da Lei nº 14.133/2021, desde que haja justificativa técnica e autorização da Administração.

11.1.1. A possibilidade de prorrogação fundamenta-se na natureza continuada dos serviços associados ao objeto (ver item 1.6), especialmente:

11.1.1.1. no Lote 1, quanto aos serviços de suporte técnico da solução de ADC, indispensáveis à manutenção da infraestrutura crítica de tecnologia da informação do TJCE;

11.1.1.2. no Lote 2, quanto à prestação contínua da solução WAF em modelo SaaS, cuja necessidade é permanente, sendo essencial à segurança das aplicações web institucionais.

11.1.2. A interrupção dos serviços descritos poderá acarretar prejuízos à continuidade das atividades institucionais, à disponibilidade dos sistemas e à segurança da informação, caracterizando, assim, a necessidade de sua manutenção contínua ao longo do tempo.

11.2. A definição desses prazos observa o art. 105 da Lei nº 14.133/2021, garantindo compatibilidade com o Plano Plurianual (PPA) e com a disponibilidade orçamentária durante toda a execução. Conforme a Lei Estadual nº 18.662/2023 (PPA 2024–2027), as ações orçamentárias associadas são:

11.2.1. Lote 1: Ação 11470 – Desenvolvimento da Infraestrutura de TI – FERMOJU (1º Grau) e Ação 11473 – Desenvolvimento da Infraestrutura de TI – FERMOJU (2º Grau), destinadas ao pagamento de despesas de investimento para desenvolvimento e aperfeiçoamento da infraestrutura tecnológica.

11.2.2. Lote 2: Ação 20511 – Apoio ao Desenvolvimento da Prestação Jurisdicional na Área de TI – FERMOJU (1º Grau) e Ação 20512 – Apoio ao Desenvolvimento da Prestação Jurisdicional na Área de TI – FERMOJU (2º Grau), destinadas ao pagamento de despesas com contratações de pessoas jurídicas para apoio à prestação jurisdicional na área de tecnologia da informação.

11.2.3. O prazo de 60 meses para o Lote 1 justifica-se pelo investimento necessário, pela natureza de infraestrutura crítica e pela necessidade de garantir continuidade, estabilidade operacional e desempenho às funções essenciais de conectividade do TJCE. A análise de práticas de mercado mostra que vigências de 60 meses são predominantes em contratações similares, como as realizadas no TJRO, STJ, TRF3/CJF e TRF1, reforçando que o prazo adotado segue o padrão de referência utilizado por diversos órgãos da Administração Pública.

11.2.4. Para o Lote 2, o prazo de 36 meses está alinhado ao modelo de contratação SaaS, às características de consumo variável por franquia e ao ciclo tecnológico das soluções de proteção de aplicações web, mantendo equilíbrio entre evolução tecnológica e previsibilidade contratual. Esse prazo também acompanha o padrão adotado por órgãos como TRTs e SERPRO, não

havendo vantagem financeira comprovada na adoção de períodos maiores, já que se trata de serviço e não foram identificados descontos progressivos que justificassem vigência superior.

11.2.5. Devido à importância destes serviços e no intuito de sempre melhor atender às demandas de manutenção, suporte e garantia inerentes a solução a ser adquirida, sobretudo os utilizados pelo TJCE, além dos significativos acréscimos de serviços em relação ao escopo de trabalho atual em função das demandas de crescimento e ampliação dos serviços judiciais e administrativos.

11.2.6. Devido à importância destes serviços e no intuito de sempre melhor atender às demandas de manutenção, de suporte e de garantia, inerentes à solução a ser adquirida, além dos significativos acréscimos de serviços em relação ao escopo de trabalho atual, em função das demandas de crescimento e ampliação dos serviços judiciais e administrativos, e a imperiosidade da sua prestação ininterrupta em face do desenvolvimento habitual das atividades administrativas, sob pena de prejuízo ao interesse público, denota-se necessária a contratação pelo tempo indicado, conforme descrito neste documento.

11.2.7. Em conformidade com o art. 6º, inciso XXIII, da Lei nº 14.133/2021, o Termo de Referência deve especificar a possibilidade de prorrogação contratual, quando for o caso, desde que observadas as condições legais. Em conformidade com os arts. 106 e 107 da Lei nº 14.133/2021, o contrato poderá ser prorrogado por até dez anos. A prorrogação poderá ocorrer sucessivamente, não necessariamente pelo mesmo período, desde que atendidas as condições legais e que a continuidade da execução do contrato seja vantajosa para a Administração Pública, considerando fatores como a eficiência, a economicidade e a disponibilidade orçamentária. A decisão de prorrogação será formalizada por meio de aditivo contratual, com a devida justificativa e observância dos requisitos legais aplicáveis.

11.3. O contrato oferecerá maior detalhamento das regras que serão aplicadas em relação à vigência, prorrogação, eventuais renovações e hipóteses de rescisão, conforme disposições legais e regulamentares aplicáveis.

12. GARANTIA DA CONTRATAÇÃO

12.1. A **CONTRATADA** prestará garantia de execução do contrato, conforme artigos 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% (cinco por cento) sobre o valor do contrato e com abrangência temporal equivalente à duração do contrato acrescida de 90 (noventa) dias.

12.1.1. A parte adjudicatária terá prazo de um mês, contado da data de homologação da licitação, para sua apresentação, que deve ocorrer antes da assinatura do contrato.

12.2. Em contratos que haja sido exigida garantia, a execução dos serviços não poderá ser iniciada antes de confirmada a garantia prestada.

12.3. Demais cláusulas em relação à garantia da contratação constarão no contrato.

13. SUBCONTRATAÇÃO E PARTICIPAÇÃO DE CONSÓRCIOS

13.1. A admissão de consórcio de empresas em licitações públicas constitui faculdade discricionária da Administração, devendo ser devidamente motivada, conforme previsto na legislação vigente.

13.2. No presente caso, considerando que o objeto da contratação consiste na prestação de serviços comuns de Tecnologia da Informação e Comunicação (TIC), com características homogêneas e amplamente ofertados no mercado, bem como que não se trata de contratação de grande vulto ou de elevada complexidade que exija a associação de empresas para sua execução, verifica-se a existência de diversos fornecedores aptos a executar o objeto de forma individual.

13.3. Dessa forma, entende-se que a participação de empresas em consórcio não se mostra necessária para assegurar a competitividade do certame, podendo inclusive dificultar a gestão contratual e a

responsabilização das contratadas. Assim, não será admitida a participação de empresas em consórcio ou cooperativas.

13.4. Quanto à execução contratual, não será admitida a subcontratação dos serviços previstos neste Termo de Referência, em razão da natureza crítica e estratégica das atividades relacionadas à operação, suporte e atendimento aos usuários de Tecnologia da Informação e Comunicação (TIC) do TJCE.

13.5. A execução direta pela CONTRATADA é necessária para assegurar:

13.5.1. a padronização e a qualidade dos serviços, em conformidade com os níveis mínimos de desempenho estabelecidos contratualmente;

13.5.2. a rastreabilidade das atividades executadas e a responsabilização direta da contratada por eventuais falhas ou não conformidades;

13.5.3. a preservação da segurança da informação, especialmente em ambientes que envolvem dados institucionais e sistemas críticos do Tribunal;

13.5.4. a adequada integração com os processos internos do TJCE, que demandam alinhamento metodológico e conhecimento dos fluxos operacionais da instituição;

13.5.5. maior efetividade na gestão e fiscalização do contrato.

13.6. Ressalta-se que a vedação à subcontratação encontra respaldo no art. 122 da Lei nº 14.133/2021, desde que devidamente motivada no planejamento da contratação, conforme entendimento do Tribunal de Contas da União no Acórdão nº 2450/2025 – Plenário.

13.7. A presente decisão foi fundamentada nas análises realizadas no Estudo Técnico Preliminar e na avaliação das alternativas de solução disponíveis no mercado, que evidenciaram a viabilidade de execução integral do objeto por fornecedor único, sem prejuízo à competitividade do certame.

13.8. Assim, considerando os riscos operacionais, de segurança da informação e de governança envolvidos na execução do objeto, conclui-se que a execução direta pela CONTRATADA é a alternativa que melhor atende ao interesse público.

14. DO REAJUSTE DE PREÇOS

14.1. Os preços contratados poderão ser reajustados, observado o interregno mínimo de 12 (doze) meses, contado a partir da data-base vinculada ao orçamento estimado da contratação, correspondente à data de finalização/assinatura da pesquisa de preços que fundamentou o valor estimado da contratação, com o objetivo de preservar o equilíbrio econômico-financeiro do contrato, nos termos da legislação vigente.

14.2. O reajuste será calculado com base na variação do Índice de Custos de Tecnologia da Informação – ICTI, divulgado pelo Instituto de Pesquisa Econômica Aplicada (IPEA).

14.3. Na hipótese de extinção, substituição ou inadequação do índice originalmente estabelecido, poderá ser adotado outro índice oficial que melhor represente a variação dos custos do objeto contratado, mediante justificativa da Administração.

14.4. O cálculo do reajuste será realizado mediante a aplicação da variação acumulada do índice no período, incidente sobre os valores contratuais vigentes à época da concessão do reajuste.

14.5. O reajuste deverá ser solicitado formalmente pela CONTRATADA, após o decurso do período mínimo previsto, mediante apresentação da respectiva memória de cálculo.

14.6. Caso a variação acumulada do índice no período seja negativa, os valores contratuais serão

ajustados proporcionalmente mediante aplicação do respectivo índice.

14.7. A formalização do reajuste ocorrerá por apostilamento ou termo aditivo, conforme o caso, observados os procedimentos administrativos aplicáveis.

15. DOS CRITÉRIOS DE SELEÇÃO DO CONTRATADA

15.1. **Regime, tipo e modalidade da licitação**

15.1.1. O PRESTADOR DE SERVIÇOS será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL POR LOTE.

15.2. **Justificativa para a aplicação do direito de preferência e margens de preferência**

15.2.1. Nos termos do art. 48, inciso III, da Lei Complementar nº 123/2006, a Administração Pública deverá estabelecer, em licitações para aquisição de bens ou contratação de serviços de natureza divisível, cota de até 25% (vinte e cinco por cento) do objeto para contratação exclusiva de microempresas e empresas de pequeno porte (ME/EPP).

15.2.2. Todavia, conforme previsto no art. 49, inciso III, da Lei Complementar nº 123/2006, o tratamento diferenciado poderá deixar de ser aplicado quando não for vantajoso para a Administração Pública ou quando puder comprometer o conjunto ou complexo do objeto a ser contratado, hipótese que deve ser devidamente justificada no planejamento da contratação.

15.2.3. No presente caso, a contratação encontra-se estruturada em dois lotes distintos, correspondentes às soluções de Application Delivery Controller (ADC) e Web Application Firewall (WAF).

15.2.4. Cada lote corresponde a uma solução tecnológica completa, cuja execução exige fornecimento, implantação, configuração, suporte técnico especializado e gestão operacional de forma integrada, não sendo recomendável sua fragmentação interna entre múltiplos fornecedores.

15.2.5. A fragmentação interna dos lotes ou a aplicação de cotas para ME/EPP poderia gerar multiplicidade de responsabilidades técnicas, aumento da complexidade de gestão contratual e dificuldades na identificação de responsabilidades em caso de falhas operacionais ou incidentes de segurança.

15.2.6. Ademais, as soluções de ADC e WAF constituem componentes críticos da infraestrutura de disponibilidade e segurança das aplicações institucionais do Tribunal, sendo responsáveis pelo processamento, inspeção e proteção do tráfego de rede destinado aos sistemas institucionais.

15.2.7. A execução dessas soluções exige gestão unificada de configuração, políticas de segurança, atualizações tecnológicas e suporte técnico especializado, o que torna tecnicamente inadequada a fragmentação da contratação sem prejuízo à eficiência operacional, à segurança da informação e à continuidade dos serviços.

15.2.8. Nesse contexto, verifica-se que a aplicação do tratamento diferenciado previsto no art. 48, inciso III, da Lei Complementar nº 123/2006 poderia comprometer o conjunto do objeto contratado, enquadrando-se na exceção prevista no art. 49, inciso III, da referida norma.

15.2.9. Ressalta-se ainda que as soluções de Application Delivery Controller (ADC) e Web Application Firewall (WAF) atuam diretamente na camada de disponibilidade e proteção das aplicações institucionais, sendo responsáveis pelo processamento e inspeção do tráfego de rede destinado aos sistemas do Tribunal. A fragmentação da solução entre múltiplos fornecedores poderia gerar indefinição de responsabilidades em situações de falhas operacionais, incidentes de segurança ou indisponibilidade de serviços, comprometendo a efetividade da gestão de

incidentes, o cumprimento dos níveis de serviço (SLAs) e a continuidade dos serviços digitais prestados pelo TJCE.

15.2.10. A decisão pela não aplicação da reserva de cotas para microempresas e empresas de pequeno porte foi fundamentada nas análises técnicas realizadas no Estudo Técnico Preliminar (ETP), que evidenciaram a necessidade de execução integrada e responsabilidade técnica centralizada dentro de cada lote, de modo a assegurar a eficiência operacional, a segurança da informação e a continuidade dos serviços de TIC do TJCE.

15.3. **Critérios de qualificação técnica para a habilitação**

15.3.1. Será exigido da **CONTRATADA** a comprovação e manutenção das seguintes QUALIFICAÇÕES ECONÔMICO-FINANCEIRAS:

15.3.1.1. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação, ou de sociedade simples;

15.3.1.2. certidão negativa de falência expedida pelo distribuidor da sede do PRESTADOR DE SERVIÇOS;

15.3.1.3. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando;

15.3.1.3.1. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

15.3.1.3.2. patrimônio líquido de 10% (dez por cento) do valor estimado da contratação;

15.3.1.3.3. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

15.3.1.4. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação mediante substituição dos demonstrativos contábeis pelo balanço de abertura.

15.3.1.5. Declaração do licitante, acompanhada da relação de compromissos assumidos, de que 1/12 (um doze avos) dos contratos firmados com a Administração Pública e com a iniciativa privada vigentes na data apresentação da proposta não é superior ao seu patrimônio líquido, podendo ser exigidos mais documentos para confirmação do declarado.

15.3.1.6. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo PRESTADOR DE SERVIÇOS.

15.3.2. Será exigido da **CONTRATADA** a comprovação e manutenção das seguintes QUALIFICAÇÕES TÉCNICAS:

15.3.2.1. Sociedades empresárias estrangeiras atenderão à exigência por meio da apresentação, no momento da assinatura do contrato, da solicitação de registro perante a entidade profissional competente no Brasil.

15.3.3. Será exigido da **CONTRATADA** a comprovação e manutenção das seguintes QUALIFICAÇÕES TÉCNICO-OPERACIONAIS:

15.3.3.1. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item

pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

15.3.3.2. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

15.3.3.2.1. Comprovação de que a licitante já executou contrato cujo objeto contemple quantitativo mínimo correspondente a 50% (cinquenta por cento) do previsto neste Termo de Referência, mediante apresentação de atestado(s) de capacidade técnica.

15.3.3.2.2. Será admitida a soma de atestados para fins de comprovação do quantitativo exigido, observado o limite máximo de 2 (dois) atestados referentes a serviços executados de forma concomitante.

15.3.3.2.3. Os atestados deverão demonstrar a execução de equipamentos, soluções ou serviços de natureza similar, com porte, capacidade, complexidade e relevância técnica equivalentes ou superiores ao objeto desta contratação.

15.3.3.2.4. Não serão aceitos atestados referentes à implantação ou fornecimento de soluções de capacidade inferior, menor criticidade ou sem equivalência tecnológica, nem aqueles que não possuam funcionalidades equivalentes às exigidas para as soluções de Application Delivery Controller (ADC) e Web Application Firewall (WAF).

15.3.3.2.5. Os atestados deverão descrever de forma clara a solução implantada ou operada e suas principais funcionalidades técnicas, de modo a permitir a verificação da compatibilidade com o objeto desta contratação.

15.3.3.2.6. Para fins de comprovação específica de cada lote:

15.3.3.2.6.1. Lote 1 – Appliance de ADC: deverá ser comprovada a implementação de equipamento do tipo Application Delivery Controller (ADC) com capacidade mínima de 20 Gbps (vinte gigabits por segundo) de throughput, equivalente a, no mínimo, 50% (cinquenta por cento) da capacidade prevista neste Termo de Referência.

15.3.3.2.6.2. Lote 2 – Serviço SaaS de WAF: deverá ser comprovada a implementação e operação de solução de Web Application Firewall (WAF) em modelo SaaS, com capacidade mínima comprovada de 20 TB (vinte terabytes) de tráfego mensal, equivalente a, no mínimo, 50% (cinquenta por cento) da capacidade prevista neste Termo de Referência.

15.3.3.2.7. Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da licitante.

15.3.3.2.8. O licitante deverá disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pelo TJCE, cópia do contrato que deu suporte à contratação, endereço atual do atestador e local em que foram prestados os serviços, entre outros documentos que venham a ser requisitados.

15.3.3.2.9. Os atestados deverão referir-se a serviços prestados no âmbito da atividade econômica principal ou secundária especificada no contrato social vigente.

15.3.3.2.10. Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras, desde que acompanhados de tradução juramentada para o português, salvo se comprovada a inidoneidade da entidade emissora.

15.3.4. Será exigido da **CONTRATADA** a comprovação e manutenção das seguintes QUALIFICAÇÕES TÉCNICO-PROFISSIONAIS:

15.3.5. Apresentar profissional(is) responsável(is) técnico(s) detentor(es) de atestado(s) de responsabilidade técnica por execução de serviços de características semelhantes ao objeto desta contratação, incluindo serviços de implantação, migração, configuração ou operação de soluções de ADC e/ou WAF.

15.3.6. 15.5.2. O(s) profissional(is) indicado(s) como responsável(is) técnico(s) deverá(ão) possuir certificação técnica válida emitida pelo fabricante da solução ofertada, compatível com a tecnologia a ser implementada no âmbito desta contratação.

15.3.7. 15.5.3. O(s) profissional(is) indicado(s) deverá(ão) participar da execução do objeto contratado, sendo admitida sua substituição por profissional de qualificação técnica e certificação equivalentes ou superiores, mediante prévia aprovação do TJCE.

16. RELAÇÃO DOS ANEXOS DO TERMO DE REFERÊNCIA

16.1. Anexo I – Especificação Técnica – Lote 1

16.2. Anexo II – Especificação Técnica – Lote 2

16.3. Anexo III – Termo de Nomeação de Preposto

16.4. Anexo IV – Termo de Compromisso

16.5. Anexo V – Termo de Ciência

16.6. Anexo VI – Instrumento de Medição de Resultado (IMR)

16.7. Anexo VII – TERMO DE RECEBIMENTO DEFINITIVO

16.8. Anexo VIII – TERMO DE RECEBIMENTO PROVISÓRIO

17. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

17.1.1. Compõe a equipe de planejamento para este objeto os seguintes servidores:

Equipe de Planejamento da Contratação				
Max Eduardo Vizcarra Melgar – 48994 Integrante Técnico		**Francisco José Pessoa Furtado – 8284** Integrante Administrativo		**Matheus Freire e Silva do Nascimento – 50707** Integrante Requisitante

18. APROVAÇÕES

Aprovo. Encaminha-se à Comissão Permanente de Licitação para iniciação de procedimento licitatório.

Autoridade Competente – SETIN
Denise Maria Norões Olsen – 24667

Fortaleza, na data da assinatura eletrônica.

Documento assinado eletronicamente por **MAX EDUARDO VIZCARRA MELGAR**, **Gestor de Unidade**, em 02/06/2026, às 23:53, 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 03/06/2026, às 08:48, 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 03/06/2026, às 11:46, 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 **DENISE MARIA NORÕES OLSEN**, **Gestor de Unidade**, em 03/06/2026, às 11:56, 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 **0733403** e o código CRC **8128B5E9**.

Referência: Processo nº 8515550-95.2025.8.06.0000 SEI nº 0733403

ANEXO I – ESPECIFICAÇÕES TÉCNICAS – LOTE 1
DESCRIÇÃO DOS SERVIÇOS E QUANTITATIVO

Lote 1			
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QUANTIDADE**
1	Controlador de Entrega de Aplicações (ADC)	Unidade	02
2	Suporte	Mês	57
3	Treinamento	Alunos	08
4	Instalação	Unidade	02

1. ITEM 1 - Controlador de Entrega de Aplicações (ADC)
1.1. REQUISITOS DE HARDWARE E PLATAFORMA

1.1.1. A solução deverá ser fornecida na modalidade on-premise, em hardware dedicado tipo appliance físico, com sistema operacional customizado, visando garantir maior segurança e desempenho.

1.1.2. A quantidade indicada no ITEM 1 (02 unidades) refere-se exclusivamente aos equipamentos físicos (appliances) que compõem a solução, não caracterizando soluções independentes, devendo ser fornecidos e operados como partes integrantes de uma única solução lógica de balanceamento de carga.

1.1.3. A solução deverá ser composta por, no mínimo, 02 (dois) equipamentos físicos (nós) independentes, idênticos, do mesmo fabricante, modelo e versão de hardware, devidamente licenciados, destinados à operação conjunta.

1.1.4. Não será aceita a entrega de equipamentos para operação isolada (standalone), ainda que atendam individualmente às especificações técnicas.

1.1.5. A solução deverá operar em cluster ativo-ativo, assegurando alta disponibilidade, com sincronização de estado entre os nós, incluindo tabelas de sessão, persistência e conexões ativas, de modo a evitar interrupção de sessões em caso de falha.

1.1.6. Os equipamentos devem ser projetados especificamente para aceleração e balanceamento de tráfego de aplicações, garantindo compatibilidade técnica para operação em alta disponibilidade (HA), com sincronização de estado e sessões, nos modos ativo-ativo e/ou ativo-passivo.

1.1.7. Os equipamentos deverão possuir quantidade de memória e capacidade de processamento suficiente para atendimento de todas as funcionalidades e desempenho solicitados neste documento, sem degradação de performance com todas as funcionalidades habilitadas simultaneamente.

1.1.8. Todas as interfaces fornecidas deverão estar integralmente licenciadas, habilitadas e operacionais para uso imediato, não sendo admitidas restrições por licenciamento adicional, devendo ser fornecidas com todos os acessórios necessários, incluindo transceivers ópticos originais, cabos e adaptadores.

1.1.9. A CONTRATADA será responsável pela interligação das interfaces do equipamento com os switches de núcleo da rede da CONTRATANTE, incluindo o

fornecimento, instalação e compatibilização de todos os componentes necessários ao pleno funcionamento da solução.

1.1.10. Os equipamentos deverão operar com tensão de entrada de 100 a 240V AC, com chaveamento automático, frequência de 50/60 Hz, não sendo aceitas fontes externas ao chassi.

1.1.11. Cada equipamento deverá ser fornecido com, no mínimo, dois (02) cabos de alimentação, em conformidade com a ABNT NBR 14136.

1.1.12. As fontes de alimentação deverão ser redundantes e hot-swappable, permitindo a substituição de unidade defeituosa sem interrupção do funcionamento.

1.1.13. O equipamento deverá ser fornecido com ventilação (fans) redundante, permitindo a substituição de unidade defeituosa sem interrupção do funcionamento.

1.1.14. Os equipamentos deverão ser fornecidos com todos os suportes necessários (gavetas e braços) para instalação em rack padrão de 19", com altura máxima de até 2U por equipamento.

1.1.15. A solução deverá permitir armazenamento de versões distintas de firmware em partições, com possibilidade de atualização, quando implementado em cluster com Alta Disponibilidade (HA), sem indisponibilidade do serviço.

1.1.16. Todos os equipamentos devem ser entregues com a versão de software homologada e recomendada pelo fabricante.

1.1.17. As licenças de uso de software serão adquiridas em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante ou seu representante.

1.1.18. Ao fim do contrato de garantia, a solução deverá permanecer completamente funcional, capaz de criar, customizar e gerenciar políticas e regras, gerar relatórios, manipular dashboards e demais funcionalidades operacionais, sem interrupção de tráfego ou perda de funcionalidades, sendo admitido apenas o encerramento dos serviços de atualização.

1.1.19. Todos os appliances físicos que compõem a solução devem ser do mesmo fabricante, modelo e versão de hardware, de forma a garantir padronização e interoperabilidade.

1.1.20. A solução deverá ser fornecida com todas as licenças de software e/ou hardware necessárias ao pleno funcionamento e atendimento integral de todas as funcionalidades exigidas neste documento, não sendo admitida a necessidade de aquisições adicionais.

1.2. REQUISITOS DE CAPACIDADE E DESEMPENHO

1.2.1. O equipamento deverá possuir, no mínimo, 64 (sessenta e quatro) gigabytes de memória RAM.

1.2.2. O equipamento deverá possuir capacidade mínima para processar 40 (quarenta) Gbps de throughput em Camada 7 (L7), de forma contínua, considerando o tráfego de aplicação efetivamente inspecionado e tratado pelo ADC.

1.2.3. O equipamento deverá possuir capacidade mínima de processamento de 30 (trinta) Gbps de tráfego SSL/TLS criptografado, de forma contínua, considerando o fluxo de dados após o estabelecimento da sessão criptográfica.

1.2.4. O equipamento deverá possuir capacidade mínima para manter, de forma simultânea, em condições típicas de operação:
1.2.4.1. 500.000 (quinhentas mil) requisições de camada 7 por segundo;
1.2.4.2. 50.000 (cinquenta mil) transações SSL por segundo, considerando chaves de 2048 bits.
1.2.5. O equipamento deverá possuir interfaces de rede, com respectivos transceivers ópticos originais do fabricante do ADC, do tipo SR (Short Range), destinadas à interligação com os switches de núcleo da rede da CONTRATANTE, atendendo a uma das seguintes configurações:
1.2.5.1. No mínimo, 02 (duas) portas com suporte a 40 Gbps e/ou 100 Gbps, utilizando conectores QSFP+ ou QSFP28; ou
1.2.5.2. No mínimo, 04 (quatro) portas com suporte a 25 Gbps, utilizando conectores SFP28.

1.3. REQUISITOS FUNCIONAIS

1.3.1. O licenciamento deve incluir, no mínimo, os seguintes serviços de balanceamento de carga e alta disponibilidade. Todos os serviços devem estar integrados na própria solução, não sendo permitido o uso de outro produto/equipamento para complementá-los:
1.3.2. Serviço de Balanceamento Global de Aplicações (GSLB);
1.3.2.1. Suporte a balanceamento em camadas 4 (transporte) e 7 (aplicação);
1.3.2.2. Suporte a algoritmos de distribuição (round robin, least connections, hash, response time);
1.3.2.3. Roteamento dinâmico (BGP, OSPF) e integração com protocolos de rede padrão;
1.3.2.4. Monitoramento de saúde (health-checks) de servidores e aplicações;
1.3.2.5. Mecanismos de persistência de sessão (cookie, source IP, SSL session ID);
1.3.2.6. Suporte a SSL Offloading e re-encriptação;
1.3.2.7. Suporte a alta disponibilidade em modo ativo-ativo e failover automático.
1.3.3. O sistema operacional/firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, e através de CLI (interface de linha de comando), acessando localmente, via porta de console, ou remotamente via SSH.
1.3.4. Deve possuir autocomplementação de comandos na CLI.
1.3.5. Deve possuir ajuda contextual na CLI.
1.3.6. Deve permitir o gerenciamento de todas as suas funcionalidades via CLI (Command Line Interface) ou GUI (Graphic User Interface).
1.3.7. Deve possuir um painel de visualização com informações das interfaces de rede do sistema.
1.3.8. A configuração de administração da solução deve possibilitar a utilização de perfis.
1.3.9. Deve ser possível executar e restaurar backup via interface web (GUI).
1.3.10. Deve ter a opção para criptografar o backup.

1.3.11. Deve ser possível executar e restaurar backup utilizando-se um ou mais dos seguintes protocolos: FTP ou HTTPS, SFTP ou TFTP.
1.3.12. Deve ser possível instalar um firmware alternativo em disco e inicializá-lo manualmente em caso de falha do firmware principal.
1.3.13. Deve ter suporte a RESTful API para gerenciamento de configurações.
1.3.14. Deve possuir interface de console para acesso local à configuração dos equipamentos.
1.3.15. Deve implementar mecanismo de controle de acesso RBAC (Role Based Access Control).
1.3.16. Deve possibilitar a configuração de filtros e definição de protocolos seguros para o acesso às interfaces de gerenciamento físicas ou virtuais.
1.3.17. Deve permitir a definição de, no mínimo, 4 (quatro) diferentes níveis de acesso à interface de gerência, limitando o acesso às configurações, relatórios e logs da solução.
1.3.18. Deve permitir restringir o acesso dos administradores via endereços IP confiáveis.
1.3.19. Deve suportar os seguintes métodos de autenticação dos administradores na interface administrativa: Local, RADIUS, LDAP e TACACS+.
1.3.20. Deve permitir a virtualização de serviços através da criação de instâncias virtuais independentes (contextos) de balanceamento de carga de aplicações.
1.3.21. A solução deve garantir isolamento total entre as instâncias virtualizadas, incluindo plano de controle, plano de dados, tabelas de sessão e recursos de hardware, administração, sem possibilidade de interferência entre ambientes distintos, ainda que coexistindo no mesmo appliance físico.
1.3.22. Deve possibilitar a alocação e limitação garantida de recursos para cada instância virtual, com base nos seguintes parâmetros:
1.3.22.1. L4 CPS;
1.3.22.2. L7 CPS e L7 RPS;
1.3.22.3. Quantidade de Interfaces de Rede;
1.3.22.4. Quantidade de largura de banda (Throughput);
1.3.22.5. SSL CPS e sessões concorrentes.
1.3.23. Deve permitir o gerenciamento completo, individual e independente das instâncias virtualizadas.
1.3.24. Nos casos de criação, edição, exclusão ou falhas de uma instância virtual, a disponibilidade e operação das demais instâncias virtualizadas, sob o mesmo appliance, não devem ser afetadas.
1.3.25. Deve permitir a definição de níveis de garantia de recursos para as instâncias virtuais, possibilitando a dedicação de recursos para determinados contextos.
1.3.26. Deve permitir a redistribuição dos recursos do appliance entre instâncias sem interrupção das instâncias não envolvidas e sob o mesmo appliance.
1.3.27. Deve implementar, no mínimo, 4 (quatro) instâncias/domínios virtualizados.
1.3.28. Cada instância virtual de balanceamento de carga de aplicações deve possuir:
1.3.28.1. Tabelas de roteamento isoladas e independentes;
1.3.28.2. Isolamento do tráfego de gerenciamento.

1.3.29. A interface de gerenciamento deve possuir plano de roteamento independente das interfaces de dados, não compartilhando tabela de roteamento com o tráfego de produção.
1.3.30. Deve possuir interface dedicada para gerenciamento remoto fora de banda (out-of-band), permitindo acesso equivalente à porta console física, incluindo operações de reinicialização e diagnóstico remoto.
1.3.31. Esta interface de gerência não deve ser a interface de console e não será contabilizada para o atendimento daquelas originalmente especificadas para o tráfego de dados do equipamento.
1.3.32. Deve suportar transferência remota para atualização do sistema operacional.
1.3.33. A solução de balanceamento de carga de aplicações deve prever gestão por meio de Gerência Centralizada, possibilitando a automação e orquestração da solução.
1.3.34. Não deve haver restrição no número de administradores que poderão ou deverão ter acesso à Gerência Centralizada, seja por acesso via WEB ou por software cliente específico.
1.3.35. Deve possuir capacidade de programabilidade por meio de linguagem de script para manipulação de tráfego em camada 7 e automação dos dispositivos por meio de API (Application Programming Interface) baseada em padrões abertos (ex.: REST).
1.3.36. A API deverá permitir, no mínimo:
1.3.36.1. Criação, alteração, remoção e consulta de objetos de configuração;
1.3.36.2. Coleta de métricas, eventos e estado operacional;
1.3.36.3. Integração com ferramentas de automação de mercado (ex.: Ansible, Terraform ou equivalentes);
1.3.36.4. Aplicação dinâmica de políticas de tráfego em camada 7 via API;
1.3.36.5. Envio de dados para outras aplicações usando REST call-back como resposta de eventos (webhooks);
1.3.36.6. Suporte a controle de acesso baseado em papéis (RBAC) em contas de usuário administrador via API.

1.4. REQUISITOS DE REDE

1.4.1. Deve permitir a conexão direta, em ambas as direções, a recursos de backend, ou endereços IP que estejam em redes roteadas pelo balanceamento de carga de aplicações.
1.4.2. Deve permitir a utilização de endereços IP duplicados, quando utilizados em instâncias diferentes.
1.4.3. Deve suportar os seguintes protocolos: SNTP (Simple Network Time Protocol) e/ou NTP.
1.4.4. Permitir consultas de DNS com resolução de nomes em endereços IPv4 e IPv6.
1.4.5. Deve prover as seguintes funcionalidades:
1.4.5.1. NAT (Network Address Translation), pelo menos nos tipos one-to-one e many-to-one e PAT (Port Address Translation), em modo estático e dinâmico;
1.4.5.2. NAT Bidirecional, de cliente e servidor:
1.4.5.2.1. Deve permitir a realização de NAT do IP do recurso de backend quando este iniciar uma conexão;
1.4.5.2.2. Tradução stateful de endereços de rede IPv6 para IPv4;

1.4.5.2.3. Tradução estática e stateless de endereços de rede IPv4 para IPv6.
1.4.5.3. DNS64 (Domain Name System).
1.4.5.4. DNSSEC (Domain Name System Security Extensions).
1.4.5.5. DNS autoritativo.
1.4.5.6. Assinatura DNS (DNS signing).
1.4.5.7. VRRPv2 (Virtual Router Redundancy Protocol) ou funcionalidade similar de FHRP (First Hop Redundancy Protocol).
1.4.5.8. VXLAN (Virtual Extensible LAN) (RFC 7348).
1.4.5.9. Implementar Policy Route ou PBR (Policy Based Routing) ou PBF (Policy Based Forwarding).
1.4.5.10. Implementar listas de controle de acesso (Access List e Prefix List) de camada 3 (três) e camada 4 (quatro), nos protocolos IPv4 e IPv6.
1.4.6. Suportar a definição de endereços IPv4 e IPv6 nas interfaces de comunicação.
1.4.7. Suportar, tanto em IPv4 quanto IPv6, a definição de rotas estáticas, rotas estáticas monitoradas e rotas estáticas com peso.
1.4.8. Suportar, no mínimo, os seguintes protocolos de roteamento dinâmico:
1.4.8.1. OSPF (Open Shortest Path First);
1.4.8.2. BGP v4 (Border Gateway Protocol);
1.4.9. Deve suportar recurso de BFD (Bidirectional Forwarding Detection).
1.4.10. Deve suportar recurso de QoS para garantia de banda dos serviços sensíveis que são balanceados pela solução.
1.4.11. Suportar ICMP e ICMPv6 (Internet Control Message Protocol).
1.4.12. ARP (Address Resolution Protocol) e GARP (Gratuitous Address Resolution Protocol).
1.4.13. Link Aggregation (802.3ad).
1.4.14. VLAN (Virtual Local Area Network) (802.1q).
1.4.15. A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso), passivo, ou "Sniffer" (Offline) e inline transparente (Bridge).
1.4.16. Suportar VLANs no padrão IEEE 802.1q.
1.4.17. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP) - IEEE 802.3ad.
1.4.18. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs).
1.4.19. A solução deve suportar roteamento por política (policy route).

1.5. FUNCIONALIDADES DE AUTENTICAÇÃO

1.5.1. Os usuários devem ser capazes de autenticar através do cabeçalho de autorização HTTP / HTTPS.
1.5.2. Os usuários devem ser capazes de autenticar através de formulários HTML embutidos.
1.5.3. A solução deverá ser capaz de autenticar usuários através de certificados digitais pessoais.
1.5.4. Deve possuir base local para armazenamento e autenticação de contas de usuários.

1.5.5. A solução deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS.
1.5.6. Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM.
1.5.7. A solução deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação.
1.5.8. Deve implantar serviços de Autenticação, Autorização e Contabilização (AAA - Authentication, Authorization and Accounting), utilizando os métodos:
1.5.8.1. Usuário/Senha local;
1.5.8.2. RADIUS (Remote Authentication Dial-In User Service).
1.5.9. A integração deve permitir identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
1.5.10. NTLM (NT LAN Manager).
1.5.11. Certificado de cliente.
1.5.12. Permitir integração com o serviço de diretório AD (Active Directory) para identificação de usuários e de grupos de usuários, permitindo maior granularidade por meio de controles e políticas baseadas em usuários e grupos de usuários.
1.5.13. Suportar SSO (Single-Sign-On) utilizando:
1.5.13.1. LDAP (Lightweight Directory Access Protocol);
1.5.13.2. Kerberos;
1.5.13.3. SAML 2.0 (Security Assertion Markup Language);
1.5.13.4. NTLM.

1.6. REQUISITOS DO BALANCEAMENTO DE CARGA DE APLICAÇÕES

1.6.1. A solução deve oferecer mecanismos de priorização de tráfego baseados em critérios das camadas 3 (três) a 7 (sete) do modelo OSI, permitindo tratamento diferenciado conforme endereços, protocolos, portas, atributos de aplicação ou demais informações disponíveis nas camadas citadas.
1.6.2. Deve permitir a criação de automações para execução automática de ações com base em eventos, incluindo eventos de segurança, de balanceamento de carga (SLB) e do sistema.
1.6.3. Em ambientes de balanceamento ativo-standby, deve possibilitar o gerenciamento da paridade de balanceamento de carga de aplicações através de endereço VIP (Virtual IP) onde somente o ativo deve responder.
1.6.4. Cada instância virtualizada deve possuir endereços de gerência e VIP específicos.
1.6.5. Quando implementada em alta disponibilidade, a solução deve permitir a definição de endereço físico (Mac Address) virtual único para ambas as instâncias virtualizadas operando em paridade.
1.6.6. Deve possuir Gerência dos balanceadores de carga de maneira INDIVIDUAL quanto a questão de configurações com:
1.6.6.1. Atualização de firmwares dos balanceadores de carga;
1.6.6.2. Monitoramento e estatísticas em tempo real dos servidores e virtual server;
1.6.6.3. Armazenamento de Logs dos balanceadores de carga;

1.6.6.4. Backup e restauração das configurações de cada balanceador de carga;
1.6.6.5. Informações dos balanceadores de carga;
1.6.6.6. Repositório de configuração dos balanceadores de carga de maneira INDIVIDUAL;
1.6.6.7. Repositório de certificados para aplicação aos balanceadores de carga de maneira INDIVIDUAL;
1.6.6.8. Templates de comandos para aplicação aos balanceadores de carga de maneira INDIVIDUAL;
1.6.6.9. Status de licenciamento dos balanceadores de carga;
1.6.6.10. Criação de novos servidores, virtual servers e health checks de maneira INDIVIDUAL.
1.6.7. Deve suportar todas as funcionalidades para comunicação HTTP/2 e HTTP/3.
1.6.8. Deve permitir a configuração de ambientes de balanceamento ou alta disponibilidade nos modos ativo-ativo, ativo-standby;
1.6.9. Permitir a configuração de grupo de balanceamento ou recurso de backend de backup, que deve ser ativado somente em caso de indisponibilidade do grupo ou recurso de backend ativo principal.
1.6.10. Deve ser capaz de balancear links de comunicação e servidores físicos ou virtuais com qualquer tipo de hardware, sistema operacional ou aplicação.
1.6.11. Deve permitir a total flexibilização da quantidade de tráfego encaminhada para cada um dos recursos de backend pertencentes a um mesmo grupo de balanceamento, possibilitando que hardwares com performances diferentes operem de forma conjunta.
1.6.12. Deve permitir que o VIP (Virtual IP) de um mesmo servidor virtual atenda às requisições em protocolos e portas específicas simultaneamente.
1.6.13. Nos casos de servidores virtuais que atendem simultaneamente diversos protocolos e portas, as requisições devem ser atendidas priorizando os parâmetros de protocolo e porta de comunicação TCP/UDP.
1.6.14. Deve permitir a criação de grupos de recursos de backend que devem compartilhar configurações e parâmetros definidos pelo usuário.
1.6.15. Deve permitir a operação e associação de um mesmo recurso de backend a mais de 1 (um) grupo de balanceamento simultaneamente.
1.6.16. Deve permitir que um mesmo recurso de backend atenda, simultaneamente, requisições em protocolos e portas de comunicação TCP/UDP diferentes.
1.6.17. Deve permitir a limitação de sessões por recurso de backend, evitando sobrecarga e contribuindo para estabilidade das aplicações.
1.6.18. Deve operar nos seguintes cenários:
1.6.18.1. Cliente em IPv4 e Recurso de backend em IPv4;
1.6.18.2. Cliente em IPv4 e Recurso de backend em IPv6;
1.6.18.3. Cliente em IPv6 e Recurso de backend em IPv4;
1.6.18.4. Cliente em IPv6 e Recurso de backend em IPv6.
1.6.19. Deve suportar, no mínimo, os seguintes métodos de balanceamento de carga, com possibilidade de configuração por serviço ou aplicação:
1.6.19.1. Métodos Estáticos e Ponderados:
1.6.19.1.1. Round Robin;

1.6.19.1.2. Round Robin com Peso Administrativo (Weight).
1.6.19.2. Métodos Dinâmicos:
1.6.19.2.1. Menor número de conexões;
1.6.19.2.2. Menor número de conexões com Peso Administrativo (Weight);
1.6.19.2.3. Menor tempo de resposta;
1.6.19.2.4. Menor número de requisições em camada 7 (L7);
1.6.19.2.5. Menor número de conexões por serviço (porta TCP ou UDP) com Peso Administrativo (Weight).
1.6.19.3. Métodos de persistência baseado em Hashing:
1.6.19.3.1. Políticas de persistência por Hash de IP e porta de origem;
1.6.19.3.2. Hash apenas de IP de Destino;
1.6.19.3.3. Hash de URL;
1.6.19.3.4. Hash de Domínio;
1.6.19.3.5. Políticas de persistência por Hash de Cookie.
1.6.19.4. Métodos de Monitoramento Avançado e Customizado:
1.6.19.4.1. O equipamento deverá ser capaz de encaminhar requisições com base em métricas de carga customizadas (como uso de CPU, memória ou latência de banco de dados), obtidas através de monitores de saúde externos e integrados à solução.
1.6.20. Deve efetuar técnicas de SSL Offloading, possibilitando os processos de criptografia e descriptografia, ou vice-versa, do tráfego entre clientes e servidores.
1.6.21. Deve permitir a utilização de Certificados Digitais assinados por Autoridades Certificadoras distintas para servidores virtuais e seus recursos de backend.
1.6.22. Deve suportar MTLS (Mutual Transport Layer Security).
1.6.23. A solução deve prover características de balanceamento de carga baseada nos seguintes protocolos TCP/UDP, HTTP, HTTPS, FTP atendendo os seguintes requisitos:
1.6.23.1. TCP/UDP:
1.6.23.1.1. Deve suportar a especificação de protocolo e portas de comunicação, limitando a comunicação aceita para determinados servidores virtuais;
1.6.23.1.2. Deve suportar a criação de servidores virtuais que aceitem requisições de qualquer protocolo e/ou porta de comunicação na conexão do cliente.
1.6.23.2. HTTP:
1.6.23.2.1. Deve suportar as versões 1.0, 1.1 e 2.0 do protocolo HTTP (HyperText Transfer Protocol), com suas respectivas especificidades e funcionalidades, provendo características de content filter, caching, compression, redirecionamento de URL (Uniform Resource Locator).
1.6.23.2.2. Deve suportar cache de conteúdo HTTP, permitindo armazenamento em memória e resposta direta ao cliente, com definição de políticas de cache por tipo de conteúdo, URL, cabeçalhos HTTP ou outros atributos da requisição;
1.6.23.3. HTTPS, SSL e TLS:
1.6.23.3.1. Deve ser capaz de manter e gerenciar todo o tráfego criptografado com os protocolos SSL 3.0, TLS 1.1, TLS 1.2 e TLS 1.3.
1.6.23.4. FTP:
1.6.23.4.1. Deve suportar as funcionalidades específicas do protocolo FTP.

1.6.24. Deve possibilitar a definição de persistência de sessão em comunicações de clientes com os recursos de backend, garantindo que, por determinado período, o mesmo servidor receba as requisições de determinado cliente.
1.6.25. Deve possibilitar a utilização da persistência de sessão mesmo para comunicações que utilizem criptografia.
1.6.26. A persistência de sessão deve se basear, no mínimo, nos seguintes parâmetros:
1.6.26.1. IP DE ORIGEM, operando com, no mínimo, os protocolos HTTP, HTTPS, TCP, UDP;
1.6.26.2. URL, operando com os protocolos HTTP e HTTPS;
1.6.26.3. COOKIE HTTP, operando com os protocolos HTTP e HTTPS;
1.6.26.4. SSL SESSION ID.
1.6.27. Deve permitir o encaminhamento de requisições para recursos de backend em portas TCP/UDP distintas da originalmente requisitada pelo cliente.
1.6.28. Deve suportar funcionalidade de compressão de HTTP, possibilitando a compressão de requisições e respostas.
1.6.29. A solução deve suportar processamento de cabeçalhos HTTP com tamanho mínimo de 128 KB por requisição, sem degradação de desempenho ou limitação funcional na aplicação de políticas de camada 7.
1.6.30. A solução deve permitir a limitação de conexões e requisições por endereço IP de origem, com definição de limites configuráveis por serviço ou aplicação.
1.6.31. Deve permitir o bloqueio automático e temporário de endereços IP que excedam os limites definidos, com possibilidade de configuração de tempo de retenção e critérios de liberação.
1.6.32. A solução deve suportar multiplexação de conexões TCP (connection reuse), permitindo o reaproveitamento de conexões estabelecidas com os servidores de backend, reduzindo a quantidade de conexões abertas e otimizando o uso de recursos dos servidores.
1.6.33. A solução deve suportar otimizações de protocolo TCP e UDP, permitindo ajuste de parâmetros de conexão entre cliente e servidor, visando melhoria de performance e redução de latência.

1.7. FUNCIONALIDADES DE ENCAMINHAMENTO BASEADO EM CONTEÚDO (L7 – CONTENT SWITCHING)

1.7.1. A solução deve realizar parsing completo das requisições e respostas HTTP/HTTPS, incluindo cabeçalhos e payload, permitindo inspeção, modificação e tomada de decisão baseada em qualquer campo da requisição ou resposta.
1.7.2. Deve permitir a apresentação de mensagens personalizáveis ao usuário em casos de bloqueio ou redirecionamento.
1.7.3. Deve identificar o tipo de agente utilizado pelo cliente (User-Agent), permitindo sua utilização como critério de decisão de encaminhamento.
1.7.4. Deve permitir a criação, edição ou supressão de mensagens HTTP de resposta ao cliente, incluindo páginas de autenticação (login), com base em políticas configuráveis.
1.7.5. A solução deverá possuir mecanismo de definição e execução de políticas em camada 7 (L7 Policy Engine), permitindo a aplicação de lógica condicional complexa

de forma centralizada, estruturada, de fácil manutenção e com comportamento determinístico.

1.7.6. Deve suportar a avaliação simultânea e combinada de múltiplos atributos da requisição HTTP, incluindo, no mínimo:

1.7.6.1. Nome de host, incluindo análise de cabeçalho HTTP Host, campo de autoridade (authority) e SNI (Server Name Indication) em conexões TLS;

1.7.6.2. URI, caminho (path) ou parâmetros da requisição;

1.7.6.3. Cabeçalhos HTTP padrão ou customizados (ex.: User-Agent, Accept-Language, Authorization ou outros definidos pela aplicação);

1.7.6.4. Método HTTP (GET, POST, PUT, etc.);

1.7.6.5. Esquema da requisição (HTTP ou HTTPS), incluindo identificação do protocolo em uso;

1.7.6.6. Informações de sessão ou cookies;

1.7.6.7. Endereço IP de origem ou atributos de conexão, como porta e protocolo.

1.7.7. Definição de políticas com operadores lógicos (AND, OR, NOT), incluindo agrupamento, aninhamento (nested) e controle de precedência.

1.7.8. Consolidação de múltiplas condições em uma única política lógica, evitando fragmentação excessiva de regras.

1.7.9. Mecanismo estruturado de políticas, não sendo aceito que o atendimento aos requisitos de lógica condicional complexa dependa exclusivamente do uso de expressões regulares (regex) ou da criação de múltiplas regras independentes para representar um mesmo comportamento funcional;

1.7.10. Suporte a múltiplos modos de comparação de URL e path (igualdade, prefixo, sufixo e equivalência após normalização).

1.7.11. Normalização de URL, garantindo tratamento consistente de variações equivalentes.

1.7.12. Manipulação de strings e atributos da requisição para uso em políticas.

1.7.13. Definição explícita de precedência e ordenação das políticas, com execução sequencial.

1.7.14. Execução das políticas diretamente no dataplane, sem dependência de componentes externos.

1.7.15. Aplicação e alteração de políticas sem necessidade de reinicialização ou indisponibilidade do serviço.

1.7.16. Suporte a linguagem de script ou mecanismo equivalente para extensão da lógica de políticas, permitindo tratamento avançado de requisições e respostas, incluindo manipulação condicional de fluxo, cabeçalhos e conteúdo.

1.7.17. Deve suportar reescrita de cabeçalhos HTTP, URLs e elementos de payload, de forma bidirecional (requisição e resposta).

1.7.18. Deve suportar limpeza de cabeçalhos HTTP (capacidade de inspecionar, remover ou modificar cabeçalhos HTTP em requisições e respostas, permitindo controle das informações trocadas entre cliente e servidor).

1.7.19. Deve suportar aplicação de políticas de resposta, reescrita e redirecionamento por serviço, aplicação ou grupo de serviços.

1.7.20. A solução deverá suportar segmentação virtual de tráfego por meio da criação de servidores virtuais de Content Switching, que atuem como ponto único de entrada para múltiplos serviços de backend, suportando, no mínimo, os protocolos HTTP, HTTPS, SSL e TCP.

1.7.21. Deve permitir a associação de múltiplas políticas de Content Switching a um mesmo servidor virtual, com definição explícita de prioridade numérica, e o processamento das políticas deve ocorrer de forma sequencial, respeitando a ordem de prioridade definida.

1.7.21.1. Deve permitir a associação de múltiplas políticas de requisição (Request) e de resposta (Response), diretamente no servidor virtual de Content Switching, possibilitando a definição e aplicação de ações com base em critérios definidos na camada 7 (L7), incluindo valores presentes no corpo, cabeçalhos ou demais atributos da requisição HTTP, respeitando a ordem de prioridade e precedência das políticas configuradas, bem como permitindo a execução das ações antes e/ou após a decisão de encaminhamento de tráfego, contemplando, no mínimo:

1.7.21.1.1. Redirecionamento de requisições (redirect ou responder), incluindo alteração de protocolo (ex: HTTP para HTTPS), porta ou URL;

1.7.21.1.2. Bloqueio de requisições com base em políticas definidas;

1.7.21.1.3. Geração de respostas personalizadas ao cliente, conforme critérios estabelecidos;

1.7.21.1.4. Reescrita de conteúdo, cabeçalhos ou URLs (rewrite), de forma bidirecional (requisição e resposta);

1.7.21.1.5. Aplicação de otimizações de entrega, tais como compressão ou manipulação de conteúdo.

1.7.22. A solução deve possuir mecanismo de tratamento de exceções para requisições que não correspondam a nenhuma política definida, por meio de servidor virtual padrão (default), garantindo comportamento previsível e controlado.

1.8. REQUISITOS DO BALANCEAMENTO DE LINKS DE INTERNET - LLB

1.8.1. A solução deve suportar o recurso de Link Load Balancing (LLB), permitindo o balanceamento de tráfego entre múltiplos links de internet, melhorando a disponibilidade e desempenho da infraestrutura.

1.8.2. A solução deve permitir a configuração de políticas de LLB, permitindo que o tráfego seja distribuído de forma inteligente entre diferentes links de internet, com base na carga, desempenho e disponibilidade de cada link.

1.8.3. O recurso de LLB deve permitir a configuração de monitoramento de saúde de links utilizando múltiplos métodos de verificação, incluindo ICMP, TCP e HTTP, garantindo a detecção precoce de falhas e a reconfiguração automática do tráfego, sem impacto na continuidade dos serviços.

1.8.4. A solução deve permitir a definição de políticas avançadas de LLB, com suporte a algoritmos de balanceamento como round-robin, least-connections e weighted round-robin, possibilitando uma distribuição eficiente do tráfego conforme a capacidade de cada link e garantindo a performance ideal da rede.

1.9. REQUISITOS DE GLOBAL SERVER LOAD BALANCING - GSLB

1.9.1. A solução deverá suportar balanceamento global de carga (GSLB), permitindo a distribuição de requisições entre datacenters distintos, com suporte a mecanismos de alta disponibilidade e failover automático entre sites.

1.9.2. A solução deverá monitorar os sites remotos e aplicar, no mínimo, os seguintes filtros de decisão baseados em:

1.9.2.1. Status de saúde do site (Health Check), com remoção automática de sites indisponíveis;

1.9.2.2. Persistência de sessão entre sites;

1.9.2.3. Número de conexões e sessões ativas;

1.9.2.4. Métricas de desempenho, incluindo latência (RTT) e carga de conexões;

1.9.2.5. Preferência administrativa por site;

1.9.3. A solução deverá suportar, no mínimo, os seguintes métodos de seleção:

1.9.3.1. Round Robin;

1.9.3.2. Menor tempo de resposta (Least Response);

1.9.3.3. Menor carga de conexões (Connection Load);

1.9.3.4. Seleção ponderada por site e/ou IP (Weighted Site / Weighted IP);

1.9.3.5. Ordenação por prioridade (Ordered Site/IP);

1.9.4. A solução deverá suportar a realização de GSLB de forma nativa, permitindo inclusive a replicação automatizada de configuração de GSLB entre os equipamentos ofertados;

1.9.5. A solução deverá suportar mecanismos de Disaster Recovery entre datacenters, incluindo integração com roteamento (ex.: Route Health Injection – RHI ou equivalente).

1.9.6. Deve possibilitar a definição de 1 (um) ou mais endereços IP específicos como origem na comunicação com determinados recursos de backend.

1.9.7. Deve suportar o encaminhamento do IP real do cliente ao Recurso de backend, seja alterando o IP de ORIGEM do cabeçalho TCP/UDP ou encaminhando-o através de campo específico de cabeçalho de comunicação.

1.9.8. Deve ser compatível com as diretivas de utilização do cabeçalho X-ForwardedFor.

1.9.9. Deve suportar a utilização de caching para aplicações com conteúdo estático e dinâmico.

1.10. REQUISITOS DE GERENCIAMENTO DE CERTIFICADOS

1.10.1. Deve possibilitar a criptografia fim-a-fim, entre cliente e recursos de backend.

1.10.2. Deve armazenar, de forma segura, arquivos de segurança como certificados digitais e chaves criptográficas:

1.10.2.1. Deve possibilitar a geração de chaves RSA (Rivest-Shamir-Adleman) e ECDSA (Elliptic Curve Digital Signature Algorithm);

1.10.2.2. Deve gerar chaves criptográficas RSA de, no mínimo, 2048 bits;

1.10.2.3. Deve implementar o algoritmo de hash SHA-256;

1.10.3. Deve permitir a importação e exportação de chaves, certificados de servidores, e checagem de lista de certificados revogados.

1.10.4. Deve possibilitar a criação de CSR (Certificate Signing Request) para a assinatura de Certificados Digitais.
1.10.5. Deve permitir a definição de CN (Common Name).
1.10.6. Deve permitir a integração com solução de HSM (Hardware Security Module).

1.11. REQUISITOS DE INTEGRAÇÕES

1.11.1. A solução deve permitir integração com sistemas externos de monitoramento e análise de segurança, tais como plataformas de SIEM e, quando aplicável, Sandbox, por meio de protocolos e formatos de mercado amplamente utilizados, como Syslog, CEF, ICAP ou equivalentes, possibilitando o envio e o compartilhamento de eventos e logs relevantes.
1.11.2. Deve ser possível criar regras de automação que permitam a execução de ações automaticamente, com base em eventos gerados pela solução, sem depender de intervenção humana.
1.11.3. Deve ser possível criar as triggers com, no mínimo, as seguintes condições:
1.11.3.1. Eventos do sistema;
1.11.3.2. Eventos de segurança;
1.11.3.3. Métricas do sistema;
1.11.3.4. Métricas das interfaces;
1.11.3.5. Agendamentos por (Mês, hora, dia, semana e um período);
1.11.3.6. Eventos de HA;
1.11.3.7. Métricas dos servidores balanceados (SLB – Server Load Balancing);
1.11.3.8. Deve possuir os seguintes tipos de ações:
1.11.3.8.1. SNMP Trap;
1.11.3.8.2. Notificação do evento via Email;
1.11.3.8.3. Executar um script via CLI.
1.11.4. A solução deve possibilitar integração com sistemas externos por meio do envio de requisições HTTP/HTTPS, permitindo acionamentos assíncronos (ex.: webhooks), quando suportado pelo fabricante.
1.11.5. Bloquear automaticamente endereços IP maliciosos na solução de firewall existente.
1.11.6. Deve possuir conectores com soluções de cloud pública e privada, permitindo a descoberta e visibilidade completa da infraestrutura de forma automática, com, no mínimo, os seguintes:
1.11.6.1. Amazon AWS;
1.11.6.2. Kubernetes.

1.12. REQUISITOS DE MONITORAMENTO E RELATÓRIOS

1.12.1. A solução de gerenciamento poderá ser integrada à solução de ADC e composta por demais produtos e soluções do mesmo fabricante, que deve contemplar, no mínimo, funcionalidades de administração centralizada, armazenamento e análise de logs, geração de relatórios, monitoramento, alertas e demais recursos necessários para a operação e acompanhamento da infraestrutura.

1.12.2. A solução de gerenciamento poderá ser integrada à solução de ADC e composta por demais produtos e soluções do mesmo fabricante dos equipamentos do Lote 2, devidamente licenciada para todas as funcionalidades exigidas nesta especificação e capaz de gerenciar integralmente o conjunto de equipamentos fornecidos.
1.12.3. Devem ser fornecidos todos os hardwares, softwares e licenças necessários para instalação e configuração da plataforma de gerenciamento.
1.12.4. As licenças da plataforma deverão permanecer ativas em caráter perpétuo, mantendo pleno funcionamento das funcionalidades já adquiridas, mesmo na ausência de cobertura de atualização ou garantia.
1.12.5. A CONTRATADA será responsável pela instalação física, configuração lógica, testes de aceitação e comissionamento de todos os equipamentos e componentes fornecidos, incluindo a parametrização de software, integração com os sistemas e rotinas do CONTRATANTE, verificação de conectividade e performance, e entrega da documentação técnica e registros dos testes realizados.
1.12.6. A plataforma deve disponibilizar acesso seguro via HTTPS e suportar mecanismos de controle de acesso baseados em papéis (RBAC), com perfis distintos de privilégio, incluindo no mínimo perfil somente leitura, permitindo integração com serviços externos de autenticação, tais como LDAP, RADIUS, Active Directory, API ou equivalentes.
1.12.7. A solução deve suportar ambientes multi-tenant ou equivalentes, permitindo segmentação lógica e gerenciamento hierárquico por domínios, grupos, áreas administrativas, sites ou localidades, assegurando isolamento adequado de recursos.
1.12.8. A solução deve permitir o gerenciamento de múltiplas instâncias, partições ou domínios lógicos do ADC, garantindo segregação administrativa e aplicação independente de políticas para cada instância separadamente.
1.12.9. A plataforma de gerenciamento deve oferecer administração centralizada e unificada de todas as instâncias e servidores virtuais presentes em um mesmo appliance físico ou ambiente distribuído, por meio de uma única interface. Essa interface deve permitir visualização consolidada, aplicação de configuração, monitoração, configuração para recebimento de logs, upgrade de firmware, execução de comandos e aplicação de certificado.
1.12.10. Deve permitir o cadastro de diferentes sites, localidades ou instâncias lógicas.
1.12.11. Deve permitir descoberta e gestão de dispositivos por meio de conectores ou protocolos padrão (ex.: SNMP, NETCONF, API REST ou equivalentes).
1.12.12. Deve disponibilizar painel centralizado com inventário de hardware com porcentagem de utilização da CPU, processamento total e por servidor virtual, Memória RAM, Disco dos equipamentos e estatísticas de conexões, assim como informações do nome do dispositivo, número de série, versão do firmware e o IP Conectado a gerência da solução.
1.12.13. Deve disponibilizar repositório centralizado de configurações disponível para restaurar no dispositivo ADC selecionado.
1.12.14. Através do gerenciamento integrado aos equipamentos ADC ou solução de gerenciamento, deve permitir a configuração e o gerenciamento centralizado dos objetos e políticas utilizados pelo ADC, incluindo servidores virtuais (VIPs), pools de

servidores, monitores de saúde (health checks), regras L4/L7, perfis de aplicação, perfis de balanceamento, regras de redirecionamento, certificados digitais e demais componentes necessários à entrega de aplicações.

1.12.15. A plataforma deve possibilitar o gerenciamento completo de certificados digitais empregados nos serviços publicados pelo ADC, incluindo importação, renovação, associação a serviços, armazenamento seguro de chaves privadas.

1.12.16. A solução de gerenciamento deve manter histórico de configurações, permitindo auditoria, função de backup automático através de agendamento e função de restauração para configurações anteriores.

1.12.17. A plataforma deve permitir o gerenciamento centralizado de scripts, políticas ou automatizações avançadas como: HTTP scripting, templates lógicos ou equivalentes.

1.12.18. Deve enviar alertas por e-mail, SMS, traps SNMP e Syslog, com política por severidade/categoria e destinatários configuráveis.

1.12.19. A solução deverá ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo Syslog.

1.12.20. A solução deve ter a capacidade de adicionar identificadores customizados, atrelados a valores fixos ou variáveis, nos registros Syslog antes do envio.

1.12.21. A solução deve permitir a exportação de logs, métricas e eventos via protocolos padrão, tais como Syslog, JSON ou formatos equivalentes, para integração com ferramentas externas de monitoramento, análise ou observabilidade.

1.12.22. A solução deve categorizar logs por tipo e permitir correlação por ID de sessão ou equivalente, facilitando análises de troubleshooting.

1.12.23. Deve ser capaz de efetuar registro (logging) dos comandos executados por determinado usuário e eventuais tentativas não autorizadas de execução de comandos (accounting).

1.12.24. A solução deverá permitir o registro detalhado de sessões possibilitando rastreabilidade completa para troubleshooting e auditoria, incluindo, no mínimo:

1.12.25. Endereço IP de origem;

1.12.26. Porta TCP ou UDP de origem;

1.12.27. Endereço IP de destino;

1.12.28. Porta TCP ou UDP de destino;

1.12.29. Protocolo de camada 4 (TCP ou UDP);

1.12.30. Data e hora da mensagem (timestamp);

1.12.31. Identificador único de sessão, conexão ou transação, que permita a correlação dos eventos e registros associados a uma mesma comunicação.

1.12.32. Deve ter suporte ao protocolo de monitoração SNMP v2c e SNMP v3.

1.12.33. Deve estar disponível para download a MIB (Management Information Base) privada dos equipamentos que compõem a solução.

1.12.34. Deve permitir a visualização de alertas da rede em tempo real.

1.12.35. Deve permitir a visualização dos dispositivos gerenciados online e offline.

1.12.36. Deve implementar, de forma nativa, mecanismo de monitoramento e detecção de falhas em suas fontes de alimentação.

1.12.37. A solução deve possuir interface gráfica com informações sobre o sistema tais como: cluster, hostname, número de série, modo de operação, tempo em serviço (uptime), versão do firmware e informações de licenças e assinaturas.
1.12.38. Deve permitir a definição de índices e o envio de alertas baseados na taxa de utilização de, no mínimo, os seguintes recursos:
1.12.38.1. Uso de CPU;
1.12.38.2. Uso de Memória;
1.12.38.3. Uso de disco.
1.12.39. A plataforma deve permitir o gerenciamento centralizado de perfis SSL/TLS, incluindo versões suportadas, cipher suites, parâmetros de handshake e políticas de segurança.
1.12.40. Deve possuir painéis (dashboards) específicos para a solução/ADC e instâncias lógicas.
1.12.41. Deve ter a capacidade de gerar relatórios detalhados baseados em tráfego, acessos e atividades do usuário.
1.12.42. A solução deve armazenar as informações por período configurável, permitindo análise temporal, geração de relatórios históricos e retenção de logs para análise posterior.
1.12.43. A solução deve ser capaz de monitorar e analisar a performance de aplicações web.
1.12.44. Deve possuir relatórios que permitam a identificação de eventuais ofensores do tráfego.
1.12.45. Deve possuir detalhamento do tempo de resposta total de carregamento de uma URL/página ou servidor, e correlação de métricas de uso de rede com o comportamento das aplicações.
1.12.46. Deve gerar informações que auxiliem nos processos de manutenções preventivas, troubleshooting, planejamento de capacidade e análise da experiência dos usuários no acesso às aplicações.
1.12.47. Deve permitir a criação, customização e agendamento de relatórios estatísticos e operacionais, com envio automático em formato HTML, CSV, Excel ou PDF.
1.12.48. Deve possuir funcionalidade de emissão de relatório gerencial/estatístico dos acessos em ferramenta local, remota ou através de composição com solução de relatórios do mesmo fabricante para todas as instâncias lógicas, de maneira unificada e segregada, além do Syslog ou log interno, que contenham, no mínimo:
1.12.48.1. Quantidade de acessos por VIP;
1.12.48.2. Quantidade de acessos por serviços e servidores;
1.12.48.3. Quantidade de usuários conectados;
1.12.48.4. Disponibilidade dos serviços/VIP;
1.12.48.5. Tempo de latência do cliente e servidor;
1.12.48.6. Throughput de requisição e resposta;
1.12.48.7. Transações por segundo;
1.12.48.8. Quantidade de requisições por período;
1.12.48.9. Quantidade de sessões;
1.12.48.10. Métodos de acesso HTTP (GET e POST);

1.12.48.11. Erros de aplicação;
1.12.48.12. Navegadores utilizados.
1.12.49. A plataforma deve disponibilizar API baseada em padrões de mercado, como REST/JSON ou equivalente, permitindo integração com ferramentas externas, automação de processos, orquestração e implementação de pipelines de DevOps ou CI/CD, quando aplicável.
1.12.50. A solução deve permitir integração com sistemas de monitoramento e observabilidade utilizados pelo CONTRATANTE (como Zabbix, Prometheus, Elastic, Grafana ou equivalentes), utilizando protocolos e formatos de mercado.
1.12.51. Deve ser disponibilizada documentação das APIs dos appliances que compõem a solução.
1.12.52. A solução deve registrar chamadas realizadas via API, incluindo usuário, horário, objeto modificado e resultado da operação.
1.12.53. A plataforma deve manter trilha de auditoria completa de todas as ações administrativas, incluindo autenticação, alterações de configuração, operações de implantação, modificações de objetos, uso da API e demais eventos relevantes, com retenção configurável conforme política do CONTRATANTE.
1.12.54. A solução de gerenciamento deve permitir a realização de backup e restore completos dos appliances ADC, contemplando a exportação e importação da configuração integral do dispositivo, incluindo objetos, políticas, certificados, perfis, parâmetros operacionais e demais componentes aplicáveis.
1.12.55. A plataforma deve possibilitar o agendamento de rotinas automáticas de backup, com retenção configurável conforme a política do CONTRATANTE, bem como permitir a restauração rápida e consistente dessas configurações em caso de falhas, migração ou necessidade de retorno a estados anteriores.

2. ITEM 2 - SUPORTE

2.1. O suporte técnico da CONTRATADA será prestado de forma contínua durante toda a vigência contratual, disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, iniciado a partir da emissão do Termo de Recebimento Definitivo.
2.2. O serviço contemplará, no mínimo:
2.2.1. Atendimento remoto e, quando tecnicamente necessário, atendimento on-site para diagnóstico, tratamento e solução de incidentes, falhas e degradações de desempenho;
2.2.2. Manutenção corretiva e preventiva, incluindo fornecimento de peças novas e originais, substituição de hardware e atualização de software/firmware, sem ônus adicional ao CONTRATANTE;
2.2.3. Tratamento de defeitos de fabricação, projeto, desempenho ou estabilidade operacional, com acionamento do fabricante quando aplicável;
2.2.4. Identificação de problemas de software/firmware, aplicação de patches, hotfixes ou versões atualizadas recomendadas pelo fabricante para correção de falhas e melhorias de estabilidade;
2.2.5. Apoio técnico na configuração e manutenção dos serviços L4/L7 publicados pelo ADC, incluindo criação, ajuste ou otimização de VIPs, pools, health checks, certificados

digitais e perfis operacionais, incluindo adição de novas aplicações e configuração de regras;

2.2.6. Análise mensal de avaliação estruturada de melhores práticas e configurações (Best Practice Assessment – BPA) com base no framework oficial da fabricante do ADC contratado.

2.2.7. Duas reuniões semanais de caráter técnico, com diagnóstico em tempo real por meio da visualização da console de gerenciamento do ADC, conduzidas por profissional do FABRICANTE do equipamento, certificado ou com treinamento oficial do fabricante no nível mais avançado de operação e configuração da ferramenta a ser contratada. As reuniões serão mantidas até que o BPA atinja aproximadamente 95% de conformidade das configurações com as recomendações do fabricante ou até decisão da CONTRATADA.

2.3. Esclarecimento de dúvidas relacionadas à administração, operação e melhores práticas recomendadas pelo fabricante;

2.4. Suporte à restauração e recuperação do ambiente em caso de falhas críticas, perda de configuração, corrupção de dados ou problemas que impactem a entrega das aplicações;

2.5. Apoio em processos de atualização de versão, migração de configuração, replicação entre instâncias e validação pós-mudança, quando necessário.

2.6. Os chamados deverão ser registrados via telefone, e-mail ou portal web, devendo cada atendimento possuir número único de controle, histórico de ações e classificação de criticidade.

2.7. Os chamados deverão ser atendidos por técnicos certificados pelo fabricante da solução, podendo a comprovação ser exigida a qualquer momento pelo CONTRATANTE.

2.8. O prazo de solução será contabilizado da abertura do chamado até o restabelecimento total do serviço. Soluções de contorno poderão ser aplicadas para mitigar impactos imediatos, devendo ser seguidas de solução definitiva em prazo acordado com o CONTRATANTE.

2.9. Nenhum chamado poderá ser encerrado sem anuência formal do responsável técnico do CONTRATANTE ou de profissional por ele designado.

2.10. A CONTRATADA deverá encaminhar relatório individual de cada chamado solucionado, contendo descrição detalhada, diagnóstico, procedimentos executados, validações, riscos residuais e medidas preventivas recomendadas.

2.11. As multas por descumprimento de SLA serão aplicadas sobre o valor mensal do suporte técnico, sem prejuízo das demais sanções previstas em contrato.

2.12. Todos os custos relativos a deslocamento, transporte de peças, troca de equipamentos ou envio de componentes serão de responsabilidade exclusiva da CONTRATADA.

2.13. A CONTRATADA deverá entregar relatório mensal consolidado de suporte técnico, contendo, no mínimo, os seguintes indicadores operacionais, inclusive em hipótese de não ter havido ocorrências no período:

2.13.1. quantidade de aplicações e domínios ativos;

2.13.2. quantidade de serviços, VIPs, pools e membros ativos no ADC;

2.13.3. número total de requisições L4/L7 processadas;

2.13.4. incidentes registrados, classificados por criticidade e causa raiz;
2.13.5. falhas de saúde detectadas pelos health checks;
2.13.6. eventos de indisponibilidade, degradação ou falha de configuração;
2.13.7. alertas de expiração de certificados digitais e recomendações preventivas.
2.13.8. SLAs de atendimento e solução (MTTA, MTTR), reaberturas e tendências;
2.14. O relatório mensal deverá ser disponibilizado em formato PDF e planilha Excel, podendo ser complementado com dashboard interativo (preferencialmente Power BI), com retenção mínima de 12 (doze) meses.
2.15. O relatório em formato PDF deverá seguir obrigatoriamente o documento modelo (template) que será disponibilizado pela CONTRATANTE. A utilização do template é obrigatória para garantir a padronização e preservar a identidade visual da CONTRATANTE em todos os relatórios técnicos que contenham seus dados, e não da CONTRATADA ou do FABRICANTE.
2.16. O relatório mensal deverá ser submetido à validação e aprovação formal pela CONTRATANTE. Caso necessário, a CONTRATANTE poderá solicitar alterações — inclusive inclusões ou exclusões de informações consideradas relevantes — antes da aprovação final.
2.17. O relatório será apresentado em reunião mensal dedicada, realizada via Microsoft Teams, com duração mínima de 1 (uma) hora, conduzida pelo Fiscal Técnico do CONTRATANTE e pela equipe técnica da CONTRATADA, contemplando análise dos indicadores, pendências, melhorias e pontos de atenção.

3. ITEM 3 - TREINAMENTO

3.1. Deverá ser ministrado treinamento, pela CONTRATADA, por parceiro ou instrutor certificados pelo fabricante para prestar serviços de capacitação referentes à solução de Balanceamento de Carga (ADC) adquirida.
3.2. O treinamento oficial deverá ser fornecido para, no mínimo, oito (8) participantes da equipe técnica do CONTRATANTE, nas dependências do TJCE ou na modalidade online, em datas e horários previamente acordados.
3.3. O treinamento poderá ser realizado de forma remota, em dias úteis, preferencialmente em turnos de até quatro (4) horas, em cronograma aprovado pelo CONTRATANTE.
3.4. O agendamento e a gravação das sessões serão conduzidos pelo Fiscal Técnico do contrato, por meio da ferramenta Microsoft Teams ou equivalente, ficando o material gravado sob a guarda do CONTRATANTE para consulta futura.
3.5. O treinamento deverá ser oficial do fabricante, ministrado à equipe técnica do CONTRATANTE, com o objetivo de capacitar os servidores na operação do ADC, possibilitando total conhecimento sobre implantação, configuração, administração, monitoramento e troubleshooting da plataforma.
3.6. O treinamento deverá ter carga horária mínima de 24 (vinte e quatro) horas, distribuídas conforme aprovado pelo CONTRATANTE.
3.7. Ao final do treinamento deverá ser fornecido certificado de conclusão para cada participante, contendo carga horária, datas, grade curricular, assinatura digital do instrutor

e menção expressa de que o curso foi realizado para a equipe técnica do Tribunal de Justiça do Estado do Ceará, conforme Contrato nº XX/202X.

3.8. Membros da equipe terceirizada poderão participar como ouvintes, sem que esta participação conte para o limite de vagas contratadas e sem emissão de certificado.

3.9. A CONTRATADA deverá informar previamente os requisitos para emissão dos certificados, tais como frequência mínima e critérios de aprovação.

3.10. O treinamento deverá ser focado em habilidades práticas para configurar e gerenciar o ADC, oferecendo laboratórios oficiais ou remotos, individualizados, e material didático digitalizado em português ou inglês.

3.11. O material didático deverá incluir documentação de "as built" da solução implementada no TJCE, destacando os recursos efetivamente implantados.

3.12. Todas as certificações exigidas para os instrutores deverão ser comprovadas mediante certificado oficial, documento equivalente ou declaração do fabricante, apresentada até dez (10) dias corridos antes do início do curso.

3.13. Os conteúdos deverão ser organizados em módulos sequenciais, com exercícios práticos ao final de cada módulo.

3.14. O material didático e os equipamentos de laboratório utilizados no treinamento deverão estar na mesma versão do ADC adquirido pelo CONTRATANTE. Não será admitido o uso de material didático referente a versões de software ou hardware desatualizadas em relação às presentes no ADC contratado.

3.15. O conteúdo programático, material didático e cronograma deverão ser enviados previamente ao TJCE para aprovação.

3.16. O CONTRATANTE poderá, a seu critério, durante o curso, solicitar a substituição de instrutor ou equipamentos de laboratório, caso identifique falhas na prestação.

3.17. Caso a deficiência não possa ser sanada sem prejuízo do curso, este será suspenso e reagendado sem ônus adicional ao CONTRATANTE.

3.18. Conteúdo Programático Mínimo:

3.18.1. Conceitos de balanceamento de carga (camada 4 e 7).

3.18.2. Configuração de VIPs (Virtual IPs) e backends.

3.18.3. Métodos de balanceamento (Round Robin, Least Connections, Response Time, Hash, etc).

3.18.4. Persistência de sessão (Cookie, Source IP, SSL Session ID).

3.18.5. Terminação SSL/TLS, offloading e re-encriptação.

3.18.6. Monitoramento e health checks de serviços.

3.18.7. Integração com DNS e suporte a GSLB.

3.18.8. Gerenciamento via GUI, CLI e APIs.

3.18.9. Conteúdo avançado

3.18.10. Configuração de alta disponibilidade (HA, Active-Active, Active-Standby).

3.18.11. Balanceamento de links de internet (Link Load Balancing).

3.18.12. Integração com ambientes híbridos (on-premises/nuvem).

3.18.13. Escalabilidade e clusters de ADC.

3.18.14. Políticas de segurança aplicadas ao tráfego balanceado.

3.18.15. Troubleshooting avançado (latência, throughput, falhas de sessão).

3.18.16. Logging, geração de relatórios e auditoria.

3.19. Caso o treinamento não seja aprovado pelo CONTRATANTE quanto ao conteúdo ou capacidade do instrutor, a CONTRATADA deverá providenciar nova turma e novo instrutor, sem custos adicionais.

4. ITEM 4 - INSTALAÇÃO

4.1. PROJETO EXECUTIVO

4.1.1. A CONTRATADA deverá elaborar o Projeto Executivo da solução de Balanceamento de Carga (ADC), contendo documentação técnica suficiente para execução, testes, homologação e auditoria.

4.1.2. O Projeto Executivo deverá contemplar, no mínimo: arquitetura física e lógica; plano de endereçamento IP e tabelas de roteamento; especificação do BOM (modelos, part numbers, versões de software/firmware, licenças e prazos); plano de capacidade (ports, throughput, CPU/memória, enlaces spine/leaf); e plano de licenciamento, suporte e garantia.

4.1.3. Deverá ser entregue Plano de Migração e Cutover, contendo cronograma de execução, janelas de manutenção, checklists de pré-produção, critérios de sucesso, rollback e contingência para mínima indisponibilidade.

4.1.4. O Projeto Executivo deverá incluir roteiros de testes de conectividade, desempenho, resiliência e integração com equipamentos existentes, com definição de métricas e evidências obrigatórias.

4.1.5. O documento deverá conter Plano de Segurança e Continuidade, prevendo segmentação, segregação de tráfego, controles de acesso, resposta a incidentes e manutenção de funções críticas em cenários de falha.

4.1.6. Deverá ser incluído Plano de Automação e Integração (scripts, templates, APIs), Plano de Treinamento e Transferência de Conhecimento, Relatório de Riscos, cronograma detalhado e lista de entregáveis.

4.1.7. Todos os artefatos deverão ser entregues em formato editável e PDF, com identificação de responsável técnico e data. A aprovação do Projeto Executivo pelo CONTRATANTE será condição para o início da implantação.

4.2. GESTÃO DO PROJETO

4.2.1. A CONTRATADA deverá designar Gerente de Projeto com experiência comprovada em implantação de soluções de TI de porte equivalente.

4.2.2. O Gerente de Projeto deverá garantir a execução integral do contrato, prazos e qualidade dos serviços.

4.2.3. O Gerente de Projeto deverá elaborar e manter cronograma atualizado das atividades, ser ponto focal para comunicações com o CONTRATANTE, emitir relatórios quinzenais de acompanhamento e apoiar a emissão do Termo de Recebimento Definitivo.

4.2.4. Os custos do Gerente de Projeto e da equipe técnica deverão estar incluídos na proposta, não cabendo ônus adicional ao CONTRATANTE.

4.3. INSTALAÇÃO E MIGRAÇÃO

4.3.1. A CONTRATADA será responsável pela instalação física e lógica da solução ADC, garantindo entrega, configuração e operação conforme o Projeto Executivo aprovado.
4.3.2. A CONTRATADA deverá apresentar, para validação do CONTRATANTE, a matriz de correspondência (de/para) entre as configurações atuais e as implementadas na nova solução, contemplando todos os elementos migrados.
4.3.3. A migração deverá contemplar, no mínimo, a conversão e implementação dos seguintes elementos existentes no ambiente atual:
4.3.3.1. Servidores virtuais (VIPs), incluindo endereços IP, portas e protocolos;
4.3.3.2. Grupos de servidores (pools ou equivalentes), membros e respectivas portas;
4.3.3.3. Métodos e políticas de balanceamento de carga;
4.3.3.4. Mecanismos de persistência de sessão;
4.3.3.5. Perfis e configurações de SSL/TLS, incluindo certificados e chaves;
4.3.3.6. Regras e políticas de camada 7 (L7), incluindo content switching, reescrita (rewrite), redirecionamento (redirect) e scripts ou regras customizadas;
4.3.3.7. Políticas de segurança, incluindo listas de controle de acesso (ACLs), limitação de conexões e bloqueios;
4.3.3.8. Configurações de monitoramento (health checks);
4.3.3.9. Integrações com sistemas externos, quando aplicável.
4.3.4. A CONTRATADA deverá garantir que todas as configurações migradas mantenham equivalência funcional com o ambiente original, sendo vedada a simplificação ou eliminação de funcionalidades sem anuência formal do CONTRATANTE.
4.3.5. A implantação e configuração inicial deverá ser realizada por profissional(ais) acreditado(s) com a certificação ou treinamento oficial do fabricante no nível mais avançado relacionado à operação e configuração da ferramenta a ser contratada.
4.3.6. Antes da entrada em produção, deverão ser realizados testes de conformidade de hardware e verificação funcional, com resultados documentados e aprovados pelo CONTRATANTE.
4.3.7. Os procedimentos de instalação e migração deverão ser submetidos previamente ao CONTRATANTE, sendo obrigatória autorização expressa para execução em produção.
4.3.8. O Plano de Migração deverá detalhar fases de execução, dependências, testes, critérios de sucesso, rollback testado e checklists assinados pelas partes.
4.3.9. Integrações críticas e automações deverão ser testadas em homologação antes da aplicação em produção.
4.3.10. Durante o cutover, a CONTRATADA deverá manter comunicação contínua com a equipe do CONTRATANTE e registrar logs das atividades, entregues ao final da janela.
4.3.11. Procedimentos de rollback deverão estar prontos para execução imediata em caso de falha, com anuência conjunta das equipes técnicas.
4.3.12. A CONTRATADA deverá adotar estratégias de migração que reduzam indisponibilidades, como staged cutover, blue/green ou coexistência temporária.

4.3.13. É obrigatória a disponibilização de acesso OOBM redundante durante e após a migração.
4.3.14. Todos os testes pós-migração deverão ser realizados e documentados, incluindo conectividade ponta a ponta, performance, redundância e resiliência.
4.3.15. A CONTRATADA deverá corrigir, sem ônus adicional, quaisquer não conformidades identificadas durante a instalação e homologação.
4.3.16. Caso seja necessário, a CONTRATADA deverá executar atividades em finais de semana ou feriados, desde que previamente acordado.
4.3.17. Ao final da migração, a CONTRATADA deverá entregar relatório final, scripts versionados, runbooks de operação e relatório de lições aprendidas.
4.3.18. A emissão do Termo de Recebimento Definitivo (TRD) da solução somente ocorrerá após a conclusão integral da implantação, configuração, migração e validação de todas as aplicações e serviços da CONTRATANTE previstos no escopo, incluindo a criação e ajuste de VIPs, pools, membros, políticas de balanceamento, persistência, health checks, regras de segurança associadas e certificados digitais, bem como a realização de testes de funcionamento, disponibilidade e desempenho, com a efetiva entrada em produção, tudo devidamente validado e atestado pelo Fiscal Técnico do CONTRATANTE.

Max Eduardo Vizcarra Melgar
Integrante Técnico

ANEXO II – ESPECIFICAÇÕES TÉCNICAS – LOTE 2

DESCRIÇÃO DOS SERVIÇOS E QUANTITATIVO

Lote 2			
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QUANTIDADE**
1	Web Application Firewall (WAF) em modelo Software como Serviço (SaaS), com franquia mensal de 50 TB de tráfego inspecionado	Mês	36
2	Franquia adicional de tráfego inspecionado a ser consumido e contratado sob demanda durante a vigência contratual	TB	900
3	Proteção DNS para 1 zona	Mês	36

1. ITEM 1 – Web Application Firewall (WAF) em modelo Software como Serviço (SaaS)

1.1. A solução deve oferecer os seguintes serviços:

1.1.1. Distribuição de conteúdo de rede – CDN;

1.1.2. Firewall de aplicação web – WAF;

1.1.3. Proteção contra ataques DDoS;

1.1.4. Proteção de APIs;

Suporte a DNSSEC;

1.1.5. Gerenciamento de bots.

1.2. A solução deve oferecer os seguintes recursos:

1.2.1. Bloqueio por geolocalização;

1.2.2. Bloqueio com base no IP;

1.2.3. Proteção com base na reputação de IP ou com base na detecção de vetores de ataque alinhados ao OWASP Top 10;

1.2.4. Monitoramento conexões de clientes;

1.2.5. Armazenamento de Logs;

1.2.6. Relatórios de disponibilidade;

1.2.7. Relatórios de utilização;

1.2.8. Relatórios de Ataques;

1.2.9. Analisador de desempenho de site;

1.2.10. Regras de Rate Control por aplicação;

1.2.11. Regras de Rate Control por conexões de clientes.

1.3. Características Gerais:

1.3.1. A solução deve ser ofertada integralmente como serviço de nuvem (SaaS) do próprio fabricante, mediante licenças de subscrição. Todas as funcionalidades exigidas devem estar nativamente integradas ou organizadas em multi-stack do mesmo fornecedor.

1.3.2. Não será aceita a composição ou concatenação de módulos provenientes de terceiros, tampouco o uso de componentes Open Source para complementar a solução.

1.3.3. Não serão aceitos componentes, módulos, funcionalidades ou serviços que se encontrem em fase de desenvolvimento, testes, pré-produção, versão beta, versão preview, acesso antecipado (early access) ou denominação equivalente, ainda que disponibilizados de forma opcional ou mediante solicitação ao fabricante.

1.3.4. Todas as funcionalidades exigidas deverão estar homologadas, estáveis, plenamente suportadas pelo fabricante e disponíveis para uso em ambiente de produção no momento da contratação, com suporte técnico regular durante toda a vigência contratual.

1.3.5. A solução deve ser licenciada com franquia mensal de consumo de dados (mínimo de 50 TB/mês) e, adicionalmente, garantir largura de banda mínima de 1Gbps para inspeção e entrega de aplicações e serviços web/API no modo WAF/WAAP, independentemente da franquia contratada. A solução deve permitir a contratação de aditivos de largura de banda durante a vigência contratual.

1.3.6. A contratação em modalidade de franquia de consumo não autoriza, em nenhuma hipótese, que a solução imponha limitações técnicas ou comerciais com base em outras métricas de utilização das aplicações, tais como quantidade de requisições HTTP/HTTPS, conexões simultâneas, sessões, chamadas de API, picos de tráfego, variações de carga legítima ou métricas equivalentes. Contudo, o consumo adicional excedente ao citado no item anterior será debitado das unidades de franquia adicional conforme o Item 2 desta especificação técnica.

1.3.7. É vedada a adoção de qualquer forma de restrição de desempenho, degradação automática ("throttling"), bloqueio, fila artificial, priorização negativa ou limitação de requisições motivada por políticas internas de capacidade da plataforma, volume processado, técnicas de inspeção profunda de pacotes (DPI) ou consumo acumulado da franquia.

1.3.8. A solução deverá operar de forma a absorver picos legítimos de tráfego, inclusive durante eventos extraordinários ou situações de aumento abrupto de demanda, sem exigir ajustes emergenciais para tal, ou aquisição imediata de licenças adicionais (quando aplicável a ferramenta).

1.3.9. O processamento de tráfego legítimo deverá ocorrer integralmente, mesmo diante de variações bruscas no volume de requisições, requisições por segundo (RPS), conexões por segundo (CPS) ou cargas instantâneas atípicas. Eventuais mecanismos de controle ou mitigação deverão aplicar-se exclusivamente ao tráfego malicioso e não poderão implicar redução de performance ou degradação no atendimento das aplicações institucionais, assegurando comportamento consistente da solução independentemente das condições de carga.

1.3.10. A solução deverá ser integrada e permitir a exportação de logs a sistemas de monitoramento e correlação de eventos, incluindo Zabbix, Grafana, Kibana e Graylog, para acompanhamento de métricas, logs e dashboards operacionais, bem como com sistemas SIEM de referência no mercado mundial (presentes no Gartner), de forma a permitir o monitoramento centralizado de desempenho, disponibilidade e segurança da solução.

1.3.11. Os serviços devem ser prestados mediante uma plataforma do fabricante não intrusiva, ou seja, sem a necessidade de instalação de equipamentos no TJCE.

1.3.12. Deve estar disponível mediante apontamento do DNS da CONTRATANTE utilizando CNAMEs.
1.3.13. Os serviços contratados serão contabilizados por volume de tráfego ou throughput mensal entregue pela plataforma.
1.3.14. Será contratada uma franquia base de volume de tráfego mensal entregue pela plataforma de 50 Terabytes, ou um throughput mensal que corresponda a este volume.
1.3.15. A empresa que decidir por ofertar o serviço em throughput deverá detalhar a métrica utilizada para garantir a correspondência com o volume entregue de 50 TB mensais.
1.3.16. Deverá ser considerado para apuração do tráfego, somente o conteúdo legítimo entregue ao usuário pelos servidores de borda. Não será aceita cobrança por ataque ou por tráfego entre os servidores da rede de distribuição de conteúdo.
1.3.17. Será contratada uma franquia adicional de volume de tráfego excedente, a ser consumido após o esgotamento do tráfego mensal contratado, conforme dimensionado no Item 2.
1.3.18. Deverá prover serviço de bloqueio de acessos indevidos, visando evitar que tentativas de ataque sejam contabilizadas, para não consumir a franquia contratada pelo TJCE.
1.3.19. A CDN deverá fornecer o serviço de controle de camada IP para bloqueio ou liberação de endereços IP. Tais listas devem ser propagadas por toda a infraestrutura da CDN.
1.3.20. A CDN deverá possuir capacidade de ocultar os websites e aplicações, restringindo o acesso dos usuários diretamente na origem, fornecendo uma camada adicional de proteção, através de uma lista definida de endereços IP que têm permissão para se comunicar com a origem da aplicação.
1.3.21. A CDN deverá suportar a criação de listas de bloqueio ou liberação de sub-redes.
1.3.22. Deverá prover serviço DNS autoritativo em nuvem, visando acelerar a resolução de nomes e proteger contra ataques aos serviços de DNS do TJCE.
1.3.23. O serviço DNS deverá ser 100% compatível com DNSSEC, conforme regras do Registro.br para domínios com o sufixo JUS.BR.
1.3.24. Deverá possuir suporte a zona de pesquisa direta.
1.3.25. Deverá ser provido de serviço de detecção, identificação e gestão de robôs (botnets), de forma a proteger os websites e as aplicações do TJCE.

1.4. REDE DE DISTRIBUIÇÃO DE CONTEÚDO – CDN

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).
1.4.2. Deverá garantir entrega de conteúdo estático e dinâmico por meio de conexões criptografadas (TLS 1.2 ou superior), suportando offload SSL distribuído em todos os pontos de presença ativos.

1.4.3. Cada data center deverá possuir servidores de distribuição de conteúdo e segurança em número suficiente para manter o SLA de 99,999% de disponibilidade.
1.4.4. A CDN deverá possuir um algoritmo de roteamento dinâmico para redirecionamento do tráfego, sem prejuízo ao desempenho dos serviços, no caso de indisponibilidade de qualquer data center.
1.4.5. A CDN deverá possuir um ambiente de testes de configurações, onde seja possível aplicar todas as funcionalidades de distribuição de conteúdo e segurança, a fim de validar todas as configurações do website ou aplicação antes de publicar em produção.
1.4.6. Este ambiente deverá possuir servidores em nuvem específicos e dedicados para realização dos testes das novas configurações.
1.4.7. A área de teste das funcionalidades especificadas no quadro dos itens do Lote 2 deste artefato de Termo de Referência, deverá possuir todas as funcionalidades do ambiente de produção.
1.4.8. O ambiente deverá possuir endereços IP ou hostnames específicos que devem ser usados nos testes, possibilitando que sejam testadas todas as funcionalidades dos websites ou aplicações protegidas, apenas realizando o direcionamento do navegador do cliente para este ambiente.
1.4.9. Deverá ser possível aplicar a mesma configuração do ambiente de teste no ambiente de produção, diretamente na interface de gerência.
1.4.10. Com a solução em produção, deverá disponibilizar simultaneamente o ambiente de teste para criação e validação de novas versões de configuração, sem que a versão em produção seja afetada.
1.4.11. A solução deverá permitir o versionamento de configurações de distribuição de conteúdo/segurança ou mecanismos de controle e gestão de alterações de configuração relacionadas à distribuição de conteúdo e às políticas de segurança, permitindo validação, aplicação controlada e reversão de mudanças (rollback) quando necessário, garantindo continuidade operacional e rápida recuperação em caso de alteração indevida.
1.4.12. A CDN deverá utilizar mecanismos automáticos de direcionamento inteligente de tráfego, baseados em critérios como latência, disponibilidade, proximidade geográfica e saúde dos nós de borda, garantindo que o usuário seja atendido pelo ponto de presença com melhores condições de entrega.
1.4.13. A solução deverá suportar balanceamento global de carga e mecanismos de failover automático, incluindo integração com serviços de DNS para direcionamento resiliente de tráfego.
1.4.14. A CDN deverá ser configurada para habilitar todos os seus servidores a reconhecer o site de origem, seus conteúdos estáticos (CSS, JS, documentos, imagem, vídeo, áudio, dentre outros) e dinâmicos, tanto no Brasil quanto no exterior.
1.4.15. A CONTRATADA deverá prover aceleração e proteção para no mínimo 255 FQDNs pertencentes ao TJCE, registradas sob 1(um) domínio (tjce.jus.br).
1.4.16. A CDN deverá prover disponibilidade dos sites e tempo de carregamento das páginas inferior ao de carregamento sem o uso da CDN, independentemente da quantidade de usuários e dados acessados simultaneamente.

1.4.17. A CDN deverá garantir o desempenho dos acessos através da determinação, em tempo real, de qual servidor de rede dinâmica possui melhores condições de entrega para cada usuário do conteúdo da aplicação acessada.
1.4.18. A solução deverá permitir aplicação e propagação automática de alterações de políticas de segurança, incluindo listas de liberação e bloqueio, em toda a rede distribuída de pontos de presença, com convergência global em até 15 (quinze) minutos, garantindo consistência entre todos os nós ativos da CDN, permitindo assim a resposta a incidentes de segurança na infraestrutura do TJCE.
1.4.19. A CDN deverá poder realizar a expiração de conteúdo (purge) por URL, com suporte a wildcard ou domínio, em toda a rede, em um prazo máximo de 5 minutos.
1.4.20. A CDN deverá possuir caminhos redundantes de acesso e distribuição de conteúdo, a fim de garantir o acesso a seus serviços, bem como ao serviço de origem.
1.4.21. A CDN deverá acelerar e distribuir indistintamente quaisquer aplicações baseadas em Protocolo de Transferência de Hipertexto (Hypertext Transfer Protocol, HTTP e HTTPS), balanceando entre seus POPs, a carga das páginas de modo a garantir melhor performance.
1.4.22. Para a aceleração e distribuição de aplicações HTTPS, a CONTRATADA deverá realizar, sem custos adicionais para o TJCE, a emissão dos certificados digitais necessários para o funcionamento de endereços em SSL.
1.4.23. Após a configuração dos certificados, deverão ser realizados testes utilizando a ferramenta SSL Labs (https://www.ssllabs.com/ssltest/), na qual deverá ser obtida a qualificação "A" para todas as URLs.
1.4.24. Os Certificados Digitais Domain Validation (DV) SSL/TLS para servidores web deverão ter as seguintes especificações:
1.4.24.1. Os certificados emitidos deverão ser do tipo Domain Validation (DV) SSL/TLS para servidor web, podendo ser individualizados para cada URL implantada ou do tipo wildcard onde o certificado permite que seja adicionada segurança SSL a ilimitados sites, desde que façam parte de subdomínios de um mesmo domínio;
1.4.24.2. Todos os certificados emitidos deverão possuir o certificado raiz da autoridade certificadora dentre as que já vêm previamente instaladas e configuradas nos principais navegadores e dispositivos do mercado suportando, no mínimo: Mozilla Firefox, Google Chrome, Edge, Safari, iPhone, Android e Windows Phone;
1.4.24.3. A CONTRATADA deverá manter o certificado válido durante todo o período do contrato;
1.4.24.4. O procedimento para validação dos certificados deverá ser on-line, telefônico ou via validação de DNS;
1.4.24.5. A fornecedora deverá possuir a capacidade de configuração das cifras e da versão de TLS utilizada pelo TJCE e deverá suportar TLS 1.2 e TLS 1.3, garantindo o uso de cifras fortes com Perfect Forward Secrecy (PFS), conforme melhores práticas de mercado e recomendações de segurança vigentes;
1.4.24.6. Deverá suportar OCSP stapling, permitir a habilitação de HTTP Strict-Transport-Security (HSTS) e aplicar automaticamente atualizações de segurança relacionadas a protocolos e algoritmos criptográficos, assegurando a desativação de cifras consideradas inseguras ou obsoletas caso necessário;

1.4.24.7. Deverá possuir validação da organização emissora do certificado digital, incluindo os dados do TJCE, conforme o caso, no certificado digital;
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;
1.4.24.9. A solução deverá suportar Mutual TLS (mTLS) para aplicações web e APIs, permitindo configurar a lista de Autoridades Certificadoras (CA) de confiança, validar certificados de cliente em listas de revogação (CRL) e, opcionalmente, encaminhar o certificado completo do cliente ou atributos específicos (subject, issuer, serial, OU, entre outros) para o servidor de origem, via cabeçalhos HTTP padronizados.
1.4.25. A CDN deverá ser capaz de identificar falhas, caso haja indisponibilidade em um dos links usados no data center de origem, para contínua transmissão e entrega do conteúdo.
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;
1.4.25.2. A CDN deverá suportar a configuração de uma origem principal e outra backup (standby), que só será utilizada em caso de falha da primeira;
1.4.25.3. A solução deverá suportar configuração de múltiplos servidores de origem e possibilitar a configuração de regras em pelo menos 2 links de internet, permitindo operação em modo ativo-passivo, com definição de prioridade entre links distintos, failover automático baseado em monitoramento contínuo de saúde e retorno automático ao servidor ou link prioritário após restabelecimento da conectividade.
1.4.26. A CDN deverá permitir a seleção de argumentos de query strings e cookies para armazenamento de objetos em cache, fazendo com que o objeto armazenado em cache seja o mesmo para solicitações com características afins.
1.4.27. A CDN deverá possuir os seguintes recursos para a gestão de cache:
1.4.27.1. Suporte a não armazenagem (no store);
1.4.27.2. Deverá possuir opção para ignorar cache (bypass cache), nesse caso o conteúdo do cache não será armazenado pela CDN.
1.4.28. A solução deverá executar mecanismos de proteção em camada de aplicação diretamente na borda (edge), integrando funcionalidades de CDN, WAF e mitigação de ataques automatizados, de forma unificada e transparente à aplicação de origem.
1.4.29. A CDN deverá permitir a criação de políticas de cache que permitam não fazer cache da requisição (bypass) assim como encaminhar os cookies tal como enviados pelos usuários para os servidores de origem.
1.4.30. A CDN deverá realizar inspeção completa de corpo de requisições HTTP/HTTPS, sem limitação de tamanho.
1.4.31. Para evitar falso positivos, a CDN deverá implementar análise e inspeção de corpo de requisições, não limitando-se apenas a assinaturas.
1.4.32. A CDN deverá responder a diferentes métodos HTTP, considerando, pelo menos: GET, HEAD, POST, PUT, PATCH, DELETE e OPTIONS.

1.4.33. A CDN deverá restringir para determinado site, métodos HTTP específicos, bloqueando outros métodos que não forem habilitados.
1.4.34. A CDN deverá modificar, adicionar ou remover informações do cabeçalho HTTP durante a comunicação com os data centers de origem.
1.4.35. A CDN deverá permitir a implementação de redirecionamento HTTP otimizando a comunicação com o data center de origem.
1.4.36. A CDN deverá fornecer o serviço de geolocalização a nível de país, que permitirá o gerenciamento de listas de permissão e negação de acessos.
1.4.37. A CDN deverá realizar a entrega de qualquer formato e tipo de conteúdo nos protocolos HTTP/1.1 e HTTP/2.
1.4.38. A CDN deverá realizar a entrega do conteúdo em cache, mesmo que já expirado, caso a origem do data center esteja inacessível.
1.4.39. A CDN deverá prover aceleração através da compressão de dados (gzip) desde que suportado pelo navegador ou dispositivo utilizado pelo usuário.
1.4.40. A CDN deverá detectar as características dos dispositivos através do tráfego de rede que contempla também as informações de navegadores de Internet.
1.4.41. A CDN deverá permitir a obtenção de objetos checados a partir de outros servidores da rede, evitando assim conexão com o data center de origem.
1.4.42. A CDN deverá permitir a execução de mecanismos de validação e autorização de requisições diretamente na borda da rede (edge), por meio de token em URL, cookies, certificados digitais (mTLS), atributos HTTP ou assinatura criptográfica, definindo se o conteúdo deve ser entregue ao usuário sem necessidade de consulta à infraestrutura de origem.
1.4.43. A CDN deverá verificar que a requisição está sendo feita por um cliente, IP ou Geolocalização autorizado a ter acesso ao conteúdo armazenado.
1.4.44. A CDN deverá possuir recurso de defesa ativa imediata, uma origem cuja solicitação corresponda a um grupo de ataque definido na ação "negar" será colocado em uma caixa de penalidade durante 10 minutos.
1.4.45. A CDN deverá prover a infraestrutura necessária para a adequada prestação dos serviços indicados anteriormente, de forma escalável, automaticamente e em tempo real, independentemente da quantidade de acessos simultâneos.
1.4.46. Através do painel de monitoramento deverá subdividir e permitir a consulta de dados referente a tráfego, requisições HTTP e HTTPS, hits, exclusivamente para cada site web configurado, permitindo a geração de relatórios específicos para cada site presente na CDN para no mínimo 30 dias de histórico.
1.4.47. O painel de monitoramento deverá possuir opções para geração de filtros, possibilitando a criação de relatórios customizados por site e data.
1.4.48. O painel de monitoramento deverá permitir acompanhar o quantitativo de requisições realizadas para cada site web na CDN.
1.4.49. O painel de monitoramento deverá disponibilizar informações como: país, endereço IP, descrição da ameaça/regra que está sendo processada, método HTTP utilizado, data e hora da ocorrência da CDN. Deverá conter, informações acerca das atividades maliciosas processadas, apresentando:
1.4.49.1. Quais sites web estão sendo atacados e;

1.4.49.2. O que está sendo explorado no ataque.
1.4.50. O painel de monitoramento deverá apresentar as informações e permitir a consulta da CDN, com delay máximo de 15 minutos e de no mínimo 30 dias de dados processados.
1.4.51. O painel de monitoramento deverá apresentar e contabilizar, através de gráficos, todas as requisições de conteúdo realizadas pelo usuário final para todo e qualquer código de status HTTP/HTTPS, gerando relatórios por período, permitindo a identificação dos picos de acesso a CDN.
1.4.52. O painel de monitoramento deverá apresentar e contabilizar, através de gráficos e API, o volume de dados trafegado, e requisições entre a CDN e o usuário final para todo e qualquer código de status HTTP.
1.4.53. O painel de monitoramento deverá apresentar e contabilizar, através de gráficos e API, o volume de dados trafegado, e requisições buscadas a partir da origem ou entregues a partir dos servidores de borda da plataforma da CDN.
1.4.54. O painel de monitoramento deverá disponibilizar os Logs das informações dos servidores para download em intervalo não superior a 1 (uma) hora da CDN.
1.4.55. Deverá possibilitar o armazenamento de Logs e Exportação de Logs para fontes externas.
1.4.55.1. A solução não deverá armazenar ou processar, de forma persistente, dados pessoais desnecessários ao propósito de segurança, tais como conteúdo completo de payloads, credenciais ou dados digitados em formulários, admitindo-se apenas a coleta de endereços IP, cabeçalhos HTTP e metadados de navegação estritamente necessários à detecção de ameaças.
1.4.56. O painel de monitoramento deverá permitir o monitoramento real de navegação dos visitantes, conforme abaixo:
1.4.56.1. O sistema deverá monitorar padrões de navegação em tempo real e acionar automaticamente CAPTCHA, mediante critérios configuráveis (ex.: taxa de requisições, comportamento suspeito ou reputação de IP), para distinguir tráfego humano de bots, com registro dos eventos no painel de monitoramento.
1.4.56.2. Deverá permitir o acompanhamento em tempo real dos dados de desempenho coletados pelos beacons, fornecendo visualização de, no mínimo, as seguintes dimensões: segurança da sessão, navegador, dispositivo e localidade geográfica;
1.4.57. A CDN deverá disponibilizar via API a consulta e a alteração das configurações de cache e regras de segurança com reflexo em todos os servidores de borda da plataforma.
1.4.57.1. A solução deverá expor API REST autenticada para consulta e alteração de configurações de segurança e CDN, com autenticação baseada em tokens ou certificados, suportando Mutual TLS (mTLS) para chamadas automatizadas;
1.4.57.2. A solução deverá disponibilizar para um cliente de linha de comando (CLI) oficial de mercado ou código para ser utilizado em CLI comum de mercado. Deverá ser compatível, no mínimo com os sistemas operacionais Linux e Windows, bem como módulos ou provedores específicos para ferramentas de automação e infraestrutura como código, tais como Terraform ou Ansible.
1.4.58. A CDN deve fornecer controles de segurança adequados, incluindo, mas não limitados a: restrição de acesso administrativo a todos os serviços (administração,

entrega) por meio de um login seguro ou autenticação de dois fatores, de modo que os serviços não possam ser utilizados por terceiros não autorizados, permitindo, ainda, a criação de perfis de acesso segregados por ambiente (produção, homologação, desenvolvimento) e por tipo de recurso (CDN, WAF, API, Bot, DNS).

1.4.59. A CDN deve fornecer gerenciamento de conta, acessos de usuários, perfis de acesso, grupo de ativos (configurações, APIs) e as permissões concedidas a usuários e grupos.

1.4.60. Capacidade de dar permissões específicas a diferentes usuários ou grupos de usuários por tipos de serviços (CDN e Segurança) e suas funções.

1.4.61. Capacidade de concessão de perfis de acesso que permitam administração hierárquica dos usuários e seus perfis.

1.5. Segurança de Firewall de Aplicação - WAF

1.5.1. A solução deverá prover serviço de WAF executado diretamente na borda da rede (edge), integrado à CDN no mesmo plano de processamento, garantindo inspeção e mitigação distribuída de requisições HTTP/HTTPS em todos os Pontos de Presença, sem introdução de latência adicional ou dependência de infraestrutura externa. Deve impedir atividade maliciosa, incluindo pelo menos as seguintes funcionalidades, além de outros tipos de ataques comuns e vulnerabilidades conhecidas a serem bloqueadas:

1.5.1.1. Bloqueio por rede e IP;

1.5.1.2. Geolocalização;

1.5.1.3. Secure token;

1.5.1.4. Força-bruta via API ou via browser;

1.5.1.5. Remote file inclusion (RFI);

1.5.1.6. Directory traversal;

1.5.1.7. Directory Climbing;

1.5.1.8. SQL injection;

1.5.1.9. Cookie Poisoning;

1.5.1.10. Violações do protocolo HTTP e HTTPS;

1.5.1.11. Detecção e bloqueio de trojans e payloads maliciosos;

1.5.1.12. Ataques de Bypass e Evasão de WAF (WAF Evasion Techniques);

1.5.1.13. Ataques de Enumeration;

1.5.1.14. Exploração de CVEs recentes;

1.5.1.15. Ataques de Deserialização insegura;

1.5.1.16. Header Injection / Cache Poisoning.

1.5.2. A solução deverá suportar definição granular dos métodos HTTP, caminhos (*paths*), parâmetros permitidos, seus respectivos tipos, formatos, tamanhos máximos e estrutura das requisições, bloqueando automaticamente qualquer requisição que não esteja em conformidade com o perfil definido para a aplicação.

1.5.3. A solução deverá suportar análise contínua de tráfego e aplicação de controles adaptativos de segurança, além de validação estrutural de payloads em APIs, incluindo JSON, possibilitando a criação, aplicação e manutenção de políticas minimamente por meio de métodos, parâmetros, tipos de conteúdo, limites de tamanho, com ações de alerta ou bloqueio para requisições inválidas.

1.5.4. A solução deverá permitir definir, por aplicação ou API, a lista de códigos de resposta HTTP (status code) considerados válidos, bloqueando e registrando como evento de segurança todas as respostas que não estejam dentro dessa lista branca.
1.5.5. A solução deverá suportar o cadastro e a proteção de APIs, observando seus métodos utilizados e operações, permitindo associá-las às políticas de segurança aplicáveis e aos mecanismos de proteções.
1.5.6. A solução deverá possuir proteção completa e contínua contra as vulnerabilidades web listadas no OWASP Top 10, observando obrigatoriamente a versão mais recente publicada pelo OWASP à época da contratação, bem como todas as versões que vierem a substituí-la ou complementá-la durante a vigência do contrato.
1.5.7. A solução deverá manter, de forma automática e sem ônus adicional para a CONTRATANTE, a atualização de suas regras, assinaturas e mecanismos de detecção de acordo com as versões mais atuais do OWASP Top 10 e dos respectivos Core Rule Sets (CRS) ou mecanismos equivalentes.
1.5.8. Não será admitida a utilização exclusiva de rulesets obsoletos, descontinuados ou baseados em versões defasadas do OWASP, ainda que complementados por promessas de atualização futura.
1.5.9. A proteção deverá abranger, no mínimo, as seguintes categorias de vulnerabilidades, conforme definidas pelo OWASP Top 10 vigente:
1.5.9.1. Injection, como injeções de SQL, NoSQL e OS;
1.5.9.2. Broken Authentication and Session Management;
1.5.9.3. Cross-Site Scripting (XSS);
1.5.9.4. Insecure Direct Object References;
1.5.9.5. Security Misconfiguration;
1.5.9.6. Sensitive Data Exposure;
1.5.9.7. Missing Function Level Access Control;
1.5.9.8. Cross-Site Request Forgery (CSRF);
1.5.9.9. Using Components with Known Vulnerabilities;
1.5.9.10. Unvalidated Redirects and Forwards;
1.5.10. A solução deverá, ainda, incorporar automaticamente a proteção contra novas classes de vulnerabilidades, riscos ou categorias que venham a ser incluídas pelo OWASP durante toda a vigência contratual, independentemente de revisão formal deste Termo de Referência.
1.5.11. A solução deverá permitir a aplicação consistente de políticas de segurança entre múltiplas aplicações, suportando reutilização de regras, perfis e configurações WAF de forma centralizada, com possibilidade de replicação controlada entre ambientes distintos, assegurando padronização e governança das configurações.
1.5.12. A solução deve manter todas as assinaturas, regras e bases de detecção continuamente atualizadas, de forma automática e sem intervenção operacional, garantindo proteção imediata contra novas ameaças, vetores de ataque e técnicas emergentes.
1.5.13. A solução deve oferecer mecanismos capazes de aplicar, de forma automática, proteções específicas para vulnerabilidades recém-divulgadas (CVE), incluindo zero-day, assegurando mitigação imediata independentemente de a aplicação ter recebido ou não o

patch oficial do fabricante, e desde que este possua uma ação mitigatória possibilitada por WAF/WAAP.

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.

1.5.15. A solução deverá possuir mecanismos de proteção contra upload malicioso de arquivos, permitindo inspeção e controle de uploads, incluindo definição de restrições de tamanho e tipo de arquivos, bem como aplicação de ações configuráveis de monitoramento ou bloqueio.

1.5.16. A solução deve suportar criação e customização de regras de limites de requisições à nível de protocolo HTTP, tendo como base a aderência à regulamentações e melhores práticas, prevenindo ataques do tipo buffer overflow, DoS, e server takeover.

1.5.17. A solução deve possuir mecanismos avançados de detecção de anomalias baseados em aprendizado de máquina, capazes de analisar o comportamento dos usuários e construir automaticamente modelos de tráfego legítimo. Esses modelos devem permitir identificar desvios significativos de padrão, sinalizando e bloqueando comportamentos inesperados, requisições atípicas e tentativas de exploração sofisticadas, mesmo quando não há assinaturas prévias disponíveis.

1.5.18. A solução deve ser capaz de capturar e analisar parâmetros de requisições (como URLs, cabeçalhos e variáveis), comparar o fluxo observado e detectar ameaças emergentes, incluindo ataques de dia zero, automações maliciosas e manipulações de tráfego. A detecção deve ocorrer de forma contínua, adaptativa e sem necessidade de intervenção manual, garantindo resposta rápida a comportamentos anômalos.

1.5.19. Deverá possuir proteção contra exploração de vulnerabilidade (exploit) por meio de inspeções de regras WAF.

1.5.20. A CDN deverá fornecer o serviço de Geo Localização para permitir o bloqueio por país e redes indesejadas (Exemplo: rede TOR).

1.5.21. A CDN deverá fornecer o serviço de controle de camada IP para bloqueio ou liberação de endereços IP. Tais listas devem ser propagadas por toda a infraestrutura da Rede de Distribuição de Conteúdo.

1.5.22. A CDN deverá suportar a criação de listas de bloqueio ou liberação de sub-redes.

1.5.23. A solução deve permitir configuração de bloqueio da requisição segundo volume por IP e pela característica da requisição.

1.5.24. A CDN deverá possuir capacidade de ocultar os websites e aplicações, restringindo o acesso dos usuários diretamente na origem, fornecendo uma camada adicional de proteção, através de uma lista definida de endereços IP que têm permissão para se comunicar com a origem da aplicação.

1.5.25. Para evitar falsos positivos, a solução deverá implementar análise e inspeção de corpo de requisições, não se limitando apenas a assinaturas.

1.5.26. Deve inspecionar e monitorar todos os dados HTTP, incluindo cabeçalhos e corpo HTTP.

1.5.27. Deve validar todos os tipos de dados inseridos, incluindo: URLs, formulários, cookies e campos.

1.5.28. A CDN deverá possuir a capacidade de criar regras de segurança customizadas para lidar com situações não incluídas no conjunto de regras padrão, a fim de corrigir vulnerabilidades rapidamente.
1.5.29. A CDN deverá possuir capacidade de proteção de segurança automática, fornecendo atualizações automaticamente, a fim de detectar e mitigar ameaças mais recentes.
1.5.30. Para reduzir a ocorrência de falsos-positivos, a ferramenta deverá possibilitar uma estrutura de categorias e assinaturas de defesa WAAP através de pontuações de risco. Cada assinatura deverá ser atrelada a uma pontuação e cada categoria de assinaturas deverá ter um limite mínimo de somatória de pontos. Baseado nessa pontuação, a ferramenta deverá tomar uma ação de mitigação/bloqueio do ataque.
1.5.31. A solução de segurança deverá contar com uma inteligência de aprendizado, incluindo uso de modelos de aprendizado de máquina (machine learning), compreendendo o funcionamento de uma aplicação Web, suas URLs, parâmetros, campos de formulário, cookies, dentre outras, para aplicar corretamente as assinaturas de defesa. Estas ações deverão ser feitas a partir do aprendizado automatizado de tráfego legítimo e sem a interferência manual de configurações.
1.5.32. A solução deverá possuir a capacidade de encaminhar, em campo específico, o endereço IPv4 de origem do cliente e porta TCP de origem do cliente.
1.5.33. Em caso de utilização de protocolo IPv6 a solução deverá encaminhar o endereço IPv6 do cliente não sendo necessário o encaminhamento da porta TCP de origem do cliente.

1.6. PROTEÇÃO ANTI DDOS

1.6.1. A CDN deverá prover serviço de defesa visando mitigar os efeitos de ataques de Distributed Denial-Of-Service (DDoS), sobre o conteúdo distribuído através dos servidores de borda, evitando que estes ataques alcancem a origem dos dados.
1.6.2. Deverá oferecer mitigação contra ataques DDoS de qualquer tipo e capacidade de mitigação de 15 Tbps ou superior, sem custos adicionais para tráfego interceptado.
1.6.3. Deverá ter no mínimo 20 (vinte) pontos de presença, que poderão no mínimo serem utilizados para mitigações de ataques DDoS.
1.6.4. Deve conter POP de mitigação DDoS no Brasil.
1.6.5. A CDN deverá mitigar de forma automática e transparente ataques em camada de aplicação, rede e transporte (L7, L4 e L3), incluindo outros vetores volumétricos ou de exaustão de recursos, com absorção distribuída na infraestrutura global do provedor (POP).
1.6.6. A solução deverá preservar a disponibilidade do serviço e a entrega das aplicações durante eventos de ataque, sem necessidade de intervenção manual ou redirecionamento para infraestrutura externa.
1.6.7. A solução deverá integrar mecanismos de detecção comportamental e mitigação adaptativa de ataques em camada de aplicação (L7), correlacionando eventos de segurança e aplicando contramedidas automáticas sem impacto significativo na experiência do usuário legítimo.

1.6.8. A CDN deverá absorver e tratar as ameaças web na origem do ataque, absorvendo o tráfego malicioso e criando proteção de perímetro dentro da Internet.

1.6.9. A CDN deverá possuir proteção automática e deve suportar, no mínimo, as seguintes capacidades:

1.6.9.1. Proteção na camada de rede por meio de bloqueio geográfico e listas dinâmicas de IP maliciosos;

1.6.9.2. A solução deverá permitir controles de taxa dinâmicos e adaptativos, integrados a mecanismos de detecção comportamental e reputação de tráfego, com aplicação distribuída na borda da rede e mitigação automática de ataques de exaustão de recursos (DDoS);

1.6.9.3. Limitação do número de requisições HTTP por segundo por endereço IP;

1.6.9.4. Controle de taxa e limitação de solicitações HTTP por cliente;

1.6.9.5. Limitação do número de conexões TCP simultâneas por cliente;

1.6.9.6. Limitação do número de conexões HTTP/TCP associadas ao mesmo cookie de sessão;

1.6.9.7. Proteção de APIs mediante bloqueio geográfico, listas dinâmicas de IP e políticas específicas de rate limit;

1.6.9.8. A solução deverá suportar mecanismos de detecção e mitigação de ataques distribuídos baseados em características do *handshake* TLS e padrões de comportamento do cliente, incluindo análise de *fingerprint* criptográfico quando aplicável, possibilitando bloqueio ou limitação automática de tráfego suspeito associado a ataques;

1.6.9.9. A solução deverá suportar identificação e controle (bloqueio, limitação, etc) de tráfego com base em Autonomous System Number (ASN) de origem, com aplicação distribuída na borda da rede e possibilidade de integração com mecanismos automatizados de detecção de tráfego de rede, assegurando resposta rápida a padrões recorrentes de abuso.

1.7. PROTEÇÃO DE API

1.7.1. A CDN deverá ser capaz de proteger as APIs implantadas para aplicações com base em pelo menos:

1.7.1.1.SOAP;

1.7.1.2.XML;

1.7.1.3.APIs em JSON;

1.7.1.4.API RESTful;

1.7.2. A solução deverá ser capaz de inspecionar o tráfego criptografado com TLS 1.2, 1.3 e rastrear o comportamento de uso para identificar o uso suspeito.

1.7.3. A solução deverá ser capaz de customizar regras para as APIs gerenciadas como uma medida de segurança adicional.

1.7.4. A solução deverá ter a capacidade de proteger as APIs associadas aos sites protegidos.

1.7.5. A solução deverá permitir fornecer segurança para APIs, descobrindo os dados utilizados nestas API e permitindo a aplicação de um modelo de segurança para proteger recursos, métodos, paths, parâmetros, tipos de conteúdo e corpo das requisições, com alerta ou bloqueio de requisições que violem as restrições configuradas.

1.7.5.1. A solução deverá permitir definir, por *endpoint* de API, a lista de códigos de status HTTP esperados, registrando e bloqueando respostas que fujam do comportamento padrão definido (desvio de *baseline*).

1.7.6. A solução deve detectar e bloquear qualquer acesso a métodos não configurados na API como uma violação.

1.7.7. A solução deve oferecer suporte a provedores de gerenciamento de API, como AWS e Azure

1.7.8. A solução deverá permitir controles de taxa dinâmicos e adaptativos, integrados a mecanismos de detecção comportamental de tráfego, com aplicação distribuída na borda da rede e mitigação automática de ataques de exaustão de recursos (DDoS).

1.7.9. Implementar mecanismo de descoberta automática de API. Monitorar todo tráfego em busca novas APIs, ocultas e não declaradas.

1.7.10. Possuir na camada de API detecção avançada de anomalias (tráfego abusivo e volumétrico) relativo àquele endpoint específico atrelado com capacidade de rate limiting customizadas (bytes e quantidade de request).

1.7.11. Ser capaz de validar a autenticação do usuário via TLS mútuo (mTLS) na API.

1.7.12. A solução deverá suportar mecanismos avançados de proteção para APIs, incluindo descoberta automática de endpoints, classificação de métodos e parâmetros de proteção dos endpoints através das aplicações publicadas no WAF/WAAP.

1.7.13. Implementar mecanismos para identificar "Shadow API", ou seja, API que foram expostas pela aplicação, mas não foram aprovadas, documentadas ou homologadas.

1.8. GERENCIAMENTO DE ROBÔS

1.8.1. A solução deverá implementar recursos de identificação e mitigação de tráfego automatizado indesejado por meio das proteções de bots/robôs, com possibilidade de integração a políticas de segurança, incluindo detecção de scraping, falsificação, e Web Crawlers, e permitindo aplicação de ações de monitoramento, permissão ou bloqueio.

1.8.2. solução deverá permitir identificar e tratar tráfego de bots indesejados, identificando-os com base em tráfego de bots conhecidos/legítimos ou não.

1.8.3. Banir bots automaticamente com base na avaliação da solicitação em busca de características de um bot, como assinaturas de cabeçalho incorretas e frameworks comuns de criação de bots.

1.8.4. Responder a tráfego de bots ou com suspeita de serem gerados por bots, por meio de desafio com solicitação CAPTCHA e demais métricas que possibilitem seu tratamento e proteção do site.

1.8.5. A solução deve permitir executar a ação configurada em bots conhecidos e confiáveis. Por padrão, todos os mecanismos de busca populares predefinidos, como Google, Bing, Yahoo, Baidu e Duck Duck Go devem estar na lista de permissões;

1.8.6. Deverá possuir uma lista dinâmica de robôs já categorizados e bots conhecidos (bots confiáveis). A lista deverá ser atualizada automaticamente para incluir novos bots ou remover bots que desaparecem.

1.8.7. Deverá ser capaz de detectar imitadores de bots conhecidos, diferenciando através do cabeçalho do User-Agent a botnet real e seu imitador.

1.8.8. A solução deverá ser capaz de identificar e bloquear bots e automações maliciosas geradas por frameworks de desenvolvimento, bibliotecas HTTP, bibliotecas de serviços web e ferramentas de automação, incluindo web crawlers, rastreadores, ataques de força bruta, slow-attacks e scripts headless. Exemplos de tecnologias e agentes que devem ser detectados: Node.js, Ruby, Java, PHP, OkHttp, Crawlera, PhantomJS, entre outros.
1.8.9. Deverá ser capaz de detectar o acesso de robôs avaliando os aspectos e anomalias da requisição como assinatura de cabeçalhos incorretas, cabeçalhos fora de ordem e incompatibilidade de versão do navegador.
1.8.10. Deverá ser capaz de criar categoria de bots personalizada, permitindo que bots específicos sejam definidos como bots amigáveis.
1.8.11. Ser capaz de diferenciar entre as requisições legítimas realizadas por usuários humanos das requisições realizadas por bots, web scraping e ataques automatizados.
1.8.12. Prover defesa contra bots, possibilitando envio de desafio com solicitação CAPTCHA ou JavaScript para detectar se um usuário é legítimo ou robô.
1.8.13. Gerenciar de forma ativa as ameaças de bot realizando seu tratamento com base em assinaturas, possibilitando a criação de controles e regras padrão e customizadas, que garantam o tratamento de no mínimo os seguintes ataques:
1.8.13.1. Rate limit para consumos identificados como anormais;
1.8.13.2. Ataques de DoS e DDoS;
1.8.13.3. Ataques de preenchimento de credenciais (Credential stuffing);
1.8.13.4. Ataques de força bruta (Brute force attack e password cracking);
1.8.13.5. Extração de dados (Web Scraping).
1.8.14. Deverá ser capaz de aplicar ações de segurança para os robôs, permitindo, no mínimo, as seguintes opções:
1.8.14.1. Monitorar o acesso, para avaliação do tráfego de robôs;
1.8.14.2. Permitir o acesso;
1.8.14.3. Bloquear o acesso e retomar código de erro HTTP 403 (acesso negado);
1.8.14.4. Bloquear o acesso e retornar com mensagem customizada;
1.8.14.5. Realizar a proteção de aplicações WEB e APIs.
1.8.15. Detectar em camadas diferentes atividades de bots para proteção do ambiente.
1.8.16. Possuir diretórios de bots conhecidos com base atualizada frequentemente.
1.8.17. Permitir a parametrização de regras de prevenção a bots.
1.8.18. Contar com uma inteligência de aprendizado, incluindo uso de modelos de aprendizado de máquina (machine learning), para aplicar corretamente as assinaturas de defesa evitando causar falsos positivos. Estas ações deverão ser feitas a partir do aprendizado automatizado de tráfego legítimo e sem a interferência manual de configurações.
1.8.18.1. A solução deverá coletar telemetria detalhada para detecção de bots, incluindo informações de ambiente, navegador/dispositivo, padrões de interação com a página e o tempo entre eventos, permitindo diferenciar de forma determinística entre tráfego humano e automatizado;
1.8.18.2. A detecção e mitigação de bots não deverá depender exclusivamente de desafios baseados em CAPTCHA ou JavaScript, devendo utilizar, prioritariamente,

análise de comportamento, fingerprint de dispositivo/navegador e telemetria para classificação de automação.

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.

1.8.20. Possuir interface única de acesso, com relatórios próximos ao tempo real, de histórico e de tendências gerais e análises detalhadas de bots individuais ou outros segmentos do tráfego de bots, com intervalo de no máximo 120 segundos.

1.8.21. A solução deverá fazer análise em tempo real de 100% das sessões reais de usuários com visibilidade de toda a execução do runtime JavaScript, não sendo permitido a análise por amostragem (sampling), detecção e análise imediata e automática de comportamento suspeito, permitindo a realização da mitigação, bloqueando a execução do script e suportar aplicações SPA (Single Page Application).

1.9. SOBRE A IMPLEMENTAÇÃO

1.9.1. Os serviços técnicos especializados têm como objetivo a implantação da solução a ser adquirida por meio deste Termo de Referência, incluindo a migração das configurações, testes e ajustes necessários para que a solução funcione perfeitamente integrada ao ambiente de produção da CONTRATANTE; devendo contemplar, no mínimo, as seguintes etapas:

1.9.1.1. Planejamento;

1.9.1.2. Execução;

1.9.1.3. Homologação;

1.9.1.4. Entrega.

1.9.2. Os LICITANTES poderão agendar visitas técnicas "Presencialmente ou Remotamente", a partir da publicação do edital para conhecer as condições lógicas da rede de forma a possibilitar um dimensionamento mais preciso do trabalho a ser realizado.

1.9.3. A CONTRATADA será responsável pelo pleno funcionamento da "Infraestrutura Tecnológica" onde se encontrará hospedada a solução, devendo se responsabilizar por disponibilizar todos os esforços necessários para garantir a disponibilidade, integridade e segurança do ambiente.

1.9.4. A CONTRATADA deverá prover serviços profissionais do fabricante ou técnicos certificados pelo fabricante para execução dos serviços solicitados.

1.9.5. A CONTRATADA deverá realizar a Configuração da solução adquirida de acordo com as exigências levantadas.

1.9.6. A CONTRATADA deverá realizar toda configuração da solução de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada.

1.9.7. Demais tarefas relacionadas à solução ofertada, que porventura não estejam previstas, mas que sejam necessárias para o seu correto funcionamento, deverão ser executadas pela CONTRATADA, sem custo adicional para o TJCE.

1.9.8. A solução deverá ser configurada de modo a garantir total operabilidade com o ambiente computacional do TJCE e ser otimizada para usufruir das melhores condições em termos de desempenho e disponibilidade.

1.9.9. Todos os serviços de implantação, configuração, migração e testes deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante da solução adquirida. Em momento anterior à implantação, o CONTRATANTE poderá solicitar os comprovantes da qualificação profissional do técnico que executará os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas.
1.9.10. Definir, junto com o CONTRATANTE, quais FQDNs do TJCE receberão a proteção da solução e configuração da solução adquirida, e a ordem.
1.9.11. As FQDNs poderão ser agrupadas para implantação simultânea da solução, mediante definição em conjunto com o CONTRATANTE.
1.9.12. Configurar para cada FQDN selecionada, a CDN, a política WAF, a proteção a APIs, a política de gerenciamento de bots e a política anti DDoS.
1.9.13. Realizar todas as configurações recomendadas incluindo logs, envio de e-mails e parametrizações de relatórios.
1.9.14. Ao término dos serviços deve ser criado um relatório detalhado de todos os itens configurados no projeto (relatório as-built) redigido em português do Brasil e contendo etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução implantada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações da solução contendo no mínimo as seguintes informações:
1.9.14.1. Mapeamento atualizado das aplicações e websites do TJCE publicados externamente e protegidos com a solução;
1.9.14.2. Detalhamento das configurações implementadas no ambiente;
1.9.14.3. Procedimentos e rotinas periódicos que devem ser realizados pela equipe do TJCE para manter a solução dentro das melhores práticas indicadas pela fabricante da solução adquirida.
1.9.15. A emissão do Termo de Recebimento Definitivo (TRD) da solução somente ocorrerá após a conclusão integral da migração, configuração, validação e entrada em produção de todas as aplicações da CONTRATANTE, compreendendo os FQDNs, incluindo a aplicação das políticas de segurança, testes de funcionamento, verificação de disponibilidade, desempenho e efetiva proteção pelo WAF, devidamente atestados pelo Fiscal Técnico do CONTRATANTE.

1.10. DAS CARACTERÍSTICAS DO SUPORTE TÉCNICO

1.10.1. O início do período de suporte técnico será a partir da finalização da implementação e emissão do TRD por parte do TJCE do item 1.
1.10.2. A CONTRATADA será responsável por prover o Serviço de Suporte Técnico, devendo oferecer suporte técnico 24x7x365, ou seja, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, a fim de atender incidentes e demandas encaminhadas pelo TJCE.
1.10.3. A CONTRATADA deverá disponibilizar atendimento em português Brasileiro;
1.10.4. Deverá possuir suporte do fabricante por 36 (trinta e seis) meses, contemplando as atualizações do software (correções, “patches”, “updates” ou novas “releases”),

quando disponíveis, incluindo atualizações de segurança classificadas como críticas ou de alta severidade.

1.10.5. A CONTRATADA deverá garantir a migração, sempre que houver mudança de destino do tráfego — seja para nuvem ou para o data center local— todas as políticas, perfis de segurança, regras de WAF, proteção de APIs, mitigação DDoS e controles Anti-Bot permaneçam íntegros, funcionais e aplicados de forma consistente.

1.10.6. A CONTRATADA será responsável pela mão de obra para suporte e atendimento remoto.

1.10.7. A CONTRATADA deverá ter acesso direto e contínuo ao serviço de *Professional Services* do fabricante da solução. Esse suporte especializado deve ser acionado para tratar incidentes complexos, troubleshooting avançado, ajustes de performance, falhas estruturais, análises de anomalias, migrações, revisões arquiteturais e demais necessidades que extrapolem o suporte de primeiro e segundo nível.

1.10.8. As manutenções preventivas e corretivas serão de responsabilidade do fornecedor, sem custos adicionais ao CONTRATANTE.

1.10.9. Para prestação do Serviço de Suporte Técnico, a CONTRATADA deverá estar apta para orientar, apoiar e acompanhar as solicitações do TJCE, cobrindo minimamente o seguinte rol de atividades:

1.10.9.1. Uso, configuração e implantação da solução;

1.10.9.2. Instalação e configuração de qualquer programa, ferramenta ou extensão necessária para habilitar funcionalidades previstas na solução;

1.10.9.3. Interoperabilidade da solução com outros produtos do TJCE quando tecnicamente compatível e suportado pelo fabricante;

1.10.9.4. Diagnóstico e correção de falhas ou problemas (troubleshooting);

1.10.9.5. Elaboração de scripts ou playbooks técnicos para execução de tarefas, ajustes operacionais ou correções mitigatórias emergenciais;

1.10.9.6. Adequação da solução às melhores práticas orientadas pelo fabricante;

1.10.9.7. Aperfeiçoamento das configurações aplicadas;

1.10.9.8. Otimização da performance operacional (tuning);

1.10.9.9. Atualização (upgrade) ou reversão (downgrade) de versão;

1.10.9.10. Elaboração e personalização de relatórios gerenciais e operacionais;

1.10.9.11. Interpretação da documentação da solução;

1.10.9.12. Recuperação do ambiente em caso de panes ou perda de dados, incluindo suporte a restauração de configurações, validações pós-recuperação e garantia de consistência operacional no âmbito da plataforma da solução contratada;

1.10.9.13. Abertura de chamados com o fabricante;

1.10.9.14. Análise mensal de avaliação estruturada de melhores práticas e configurações (*Best Practice Assessment* – BPA) com base nas recomendações oficiais do fabricante do WAF contratado;

1.10.9.15. Duas reuniões semanais de caráter técnico, com diagnóstico em tempo real por meio da visualização da console de gerenciamento do WAF, conduzidas por profissional do FABRICANTE do equipamento, certificado ou com treinamento oficial do fabricante no nível mais avançado de operação e configuração da ferramenta a ser contratada. As reuniões serão mantidas até que o BPA atinja aproximadamente 95% de

conformidade das configurações com as recomendações do fabricante ou até decisão da CONTRATADA.

1.10.10. A critério do TJCE, as atividades técnicas poderão ser executadas pelo TJCE ou pela CONTRATADA. Quando executada pela CONTRATADA a mesma deverá notificar o TJCE.

1.10.11. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados, em sistema fornecido pela CONTRATADA. Esse serviço destina-se a esclarecimento de dúvidas, solicitação de configurações e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA, devendo o sistema de chamados registrar SLA, prioridade, histórico e anexos técnicos.

1.10.12. A CONTRATADA deverá apresentar, até o 8º (oitavo) dia útil de cada mês, um relatório (em formato PDF) contendo o registro de todos os chamados abertos no mês anterior, inclusive em hipótese de não ter havido ocorrências no período.

1.10.13. O relatório deverá conter, no mínimo, as seguintes informações:

1.10.13.1. Nº do chamado;

1.10.13.2. Categoria de prioridade;

1.10.13.3. Descrição do problema e da solução;

1.10.13.4. Procedimentos realizados;

1.10.13.5. Data e hora da abertura e do fechamento do chamado;

1.10.13.6. Data e hora do início e do término da execução dos serviços e;

1.10.13.7. Identificação do técnico da empresa.

1.10.14. A CONTRATADA deverá, ainda, levando-se em consideração o ambiente da CONTRATANTE, as seguintes informações no relatório mensal:

1.10.14.1. Quantidade de aplicações, domínios e subdomínios protegidos pelo WAF;

1.10.14.2. Quantidade de políticas, regras e perfis de segurança ativos (WAF, anti-bot, rate limiting, API security, entre outros, quando aplicável);

1.10.14.3. Volume total de requisições HTTP/HTTPS inspecionadas e bloqueadas, discriminadas por período;

1.10.14.4. Número de ataques detectados e mitigados, classificados por tipo (OWASP Top 10, bots, DDoS L7, exploits conhecidos, entre outros) e severidade;

1.10.14.5. Incidentes de segurança registrados, com indicação de criticidade, impacto, causa raiz e ações corretivas;

1.10.14.6. Eventos de indisponibilidade, degradação de desempenho ou falhas de configuração relacionados ao serviço de WAF;

1.10.14.7. Alertas de expiração de certificados digitais, falhas de TLS/HTTPS e recomendações preventivas;

1.10.14.8. Indicadores de desempenho e disponibilidade do serviço;

1.10.14.9. Informações de novas versões de firmwares, avisos do fabricante em relação a "bugs", novos patches, anúncios de end-of-life (EOL) e end-of-support (EOS), quando aplicáveis; incluindo avisos de segurança classificados como críticos ou de alta severidade.

1.10.14.10. Recomendações de configurações a serem executadas no ambiente, incluindo recomendações preventivas, ajustes de conformidade e melhorias alinhadas às melhores práticas do fabricante.

1.10.15. O relatório mensal deverá ser disponibilizado em formato PDF e planilha Excel, podendo ser complementado com dashboard interativo (preferencialmente Power BI), com retenção mínima de 12 (doze) meses.

1.10.16. O relatório em formato PDF deverá seguir obrigatoriamente o documento modelo (template) que será disponibilizado pela CONTRATANTE. A utilização do template é obrigatória para garantir a padronização e preservar a identidade visual da CONTRATANTE em todos os relatórios técnicos que contenham seus dados, e não da CONTRATADA ou do FABRICANTE.

1.10.17. O relatório mensal deverá ser submetido à validação e aprovação formal pela CONTRATANTE. Caso necessário, a CONTRATANTE poderá solicitar alterações — inclusive inclusões ou exclusões de informações consideradas relevantes — antes da aprovação final.

1.10.18. O relatório será apresentado em reunião mensal dedicada, realizada via Microsoft Teams, com duração mínima de 1 (uma) hora, conduzida pelo Fiscal Técnico do CONTRATANTE e pela equipe técnica da CONTRATADA, contemplando análise dos indicadores, pendências, melhorias e pontos de atenção.

1.11. DAS CARACTERÍSTICAS DO TREINAMENTO

1.11.1. A CONTRATADA deverá fornecer treinamento contemplando todos os recursos e procedimentos operacionais da solução contratada, em português do Brasil na modalidade online.

1.11.2. O treinamento fornecido deverá ser: Oficial da fabricante ou de autoria da CONTRATADA, customizado para a realidade do TJCE e aprovado pela fabricante.

1.11.3. O treinamento será solicitado sob demanda do TJCE, em datas a serem acordadas entre a CONTRATANTE e CONTRATADA.

1.11.4. O agendamento e a gravação das sessões serão conduzidos pelo Fiscal Técnico do contrato (TJCE), por meio da ferramenta Microsoft Teams.

1.11.5. A gravação do treinamento será disponibilizada e armazenada sob a guarda do TJCE, para consulta interna futura pela equipe técnica.

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.

1.11.7. O treinamento será ofertado a uma turma composta por até 8 (oito) participantes da equipe técnica do TJCE.

1.11.8. A CONTRATADA deverá emitir certificado de conclusão para cada participante da turma. O certificado deverá conter a carga horária total, as datas e horários das aulas, a grade curricular, a assinatura digital do instrutor e uma menção expressa de que o treinamento foi realizado para a equipe técnica do Tribunal de Justiça do Estado do Ceará, conforme Contrato nº XX/202X.

1.11.9. Membros da equipe técnica terceirizada do TJCE poderão participar do treinamento como ouvintes, sem que essa participação conte para o preenchimento das 8 vagas contratadas. Nesses casos, a CONTRATADA não deverá emitir certificado.

1.11.10. A CONTRATADA deverá informar previamente os requisitos obrigatórios para a emissão do certificado, tais como frequência mínima de 100% ou demais critérios de aprovação.

1.11.11. O treinamento abordará os aspectos de natureza teórica e prática, abrangendo todos os componentes da solução, sobretudo aqueles implantados no TJCE: apresentação do projeto implementado, descrição da arquitetura, descrição do portal de gerência da solução, exposição de recursos da solução, configuração de alarmes para comportamentos anômalos e emissão de relatórios, diagnóstico e resolução de problemas (troubleshooting).

1.11.12. A CONTRATADA fornecerá as informações do treinamento em material didático digitalizado, que deverá abranger a documentação de "as built" da solução, ou seja, destacará os detalhes da solução efetivamente implementada no TJCE.

1.11.13. O treinamento incluirá, mas não se limitará, o seguinte conteúdo:

1.11.13.1. Criação e administração de contas de usuários e perfis de acesso na plataforma SaaS, incluindo gestão de permissões granulares e usuários privilegiados;

1.11.13.2. Uso da console web para configuração inicial do serviço, vinculação de domínios, provisionamento de aplicações e integração com provedores de identidade (IdP) via SAML/OAuth/OpenID Connect;

1.11.13.3. Criação e ajuste de políticas de segurança na borda CDN, incluindo regras de WAF, mitigação de ataques DDoS, proteção de APIs, rate limiting e gerenciamento de bots;

1.11.13.4. Monitoramento e análise de tráfego em tempo real, inspeção de logs e eventos de segurança, interpretação de métricas de desempenho e identificação de falsos positivos;

1.11.13.5. Personalização de perfis de proteção e aplicação de templates específicos para cenários comuns (e.g., aplicações web críticas, APIs públicas, microsserviços);

1.11.13.6. Geração e interpretação de dashboards e relatórios detalhados de segurança, desempenho e conformidade, incluindo exportação de dados para auditorias e relatórios regulatórios.

1.11.14. O treinamento será ministrado por instrutor certificado pelo fabricante, com experiência prática na solução de CDN, em português, e com o material didático em inglês ou português.

1.11.15. O material didático e o software de laboratório utilizado no treinamento deverão estar na mesma versão do WAF adquirido pelo CONTRATANTE. Não será admitido o uso de material didático referente a versões de software ou hardware desatualizadas em relação aos presentes no WAF contratado.

2. ITEM 2: FRANQUIA ADICIONAL DE TRÁFEGO INSPECIONADO

2.1.1. A infraestrutura da rede deverá assegurar capacidade operacional contínua, com escalabilidade automática e em tempo real, independentemente da quantidade de

acessos simultâneos, garantindo que a largura de banda contratada permaneça disponível durante todo o período de funcionamento do serviço.

2.1.2. O painel de monitoramento deverá disponibilizar ferramenta para acompanhamento em tempo real do volume trafegado, permitindo a visualização do consumo acumulado, bem como a emissão de relatórios gerenciais por período, para fins de gestão, auditoria e planejamento.

2.1.3. Após o esgotamento da franquia nativa de tráfego disponibilizada pela solução, será utilizada a franquia adicional contratada sob demanda, correspondente ao volume excedente consumido ao longo da vigência. A cobrança desse excedente será realizada conforme a métrica comercial adotada pelo fornecedor (por TB trafegado ou modelo equivalente).

2.1.4. A franquia adicional foi estimada em **900 TB para os 36 meses de vigência**. Essa franquia não altera o caráter sob demanda do consumo excedente, o qual somente será utilizado quando houver tráfego adicional efetivo, que deve permanecer integralmente disponível 24x7, independentemente da utilização.

2.1.5. A contratação da franquia adicional possui caráter **não obrigatório**, sendo utilizada apenas se houver tráfego excedente durante a vigência contratual. A Administração não assume compromisso mínimo de consumo, nem obrigação de utilização integral do volume estimado, pagando exclusivamente pelo que for efetivamente utilizado.

2.1.6. A solução deverá permitir a configuração de alertas de consumo e limiares operacionais (thresholds), possibilitando ao TJCE acompanhar tendências de uso e adotar medidas preventivas antes de atingir a totalidade da franquia adicional.

2.1.7. A contratada deverá disponibilizar metodologia clara de contabilização do tráfego consumido (TB ou GB), considerando métricas padronizadas, incluindo intervalos de coleta, descarte de tráfego inválido, ataques e critérios de agregação, assegurando transparência no cálculo do consumo excedente.

2.1.8. É vedada qualquer forma de limitação artificial (throttling), redução de throughput, priorização degradante ou restrição de funcionalidades em decorrência do consumo da franquia adicional, devendo o desempenho permanecer constante durante todo o período contratual.

2.1.9. O TJCE poderá auditar os registros de consumo (logs, relatórios, amostras e exportações) para fins de conferência, sendo obrigatória a disponibilização dos dados brutos que subsidiaram o cálculo da franquia utilizada.

2.1.10. A existência de franquia mensal não poderá ser utilizada como justificativa para restringir o volume de requisições, exigir tiers comerciais adicionais, impor limites artificiais ou introduzir modelos de cobrança por RPS, CPS, número de chamadas API ou qualquer métrica equivalente.

3. ITEM 3: PROTEÇÃO DNS PARA 1 ZONA

3.1. A CONTRATADA deverá prover solução em nuvem para os serviços de DNS autoritativo do TJCE.

3.2. A solução deve suportar os registros DNS: A/AAAA (Address record), CNAME (Canonical Name record), MX (Mail eXchange record), NS (Name Server record), PTR

(Pointer record), SRV (Service Locator recorder), TXT (text record), CAA (Certificate Authority Authorization record).

3.3. Implementar zona de pesquisa direta (Forward/Direct DNS Lookup Zone) e reversa (Reverse Lookup Zone) para um domínio;

3.4. Os serviços fornecidos deverão ser do tipo DNSSEC (Domain Name System Security Extensions).

3.5. O serviço deverá prover disponibilidade de DNS 24x7x365, com nível de serviço de 99,999%.

3.6. A solução deverá suportar resolução DNS distribuída e resiliente, integrada aos mecanismos de balanceamento global de carga e mitigação de ataques, garantindo continuidade operacional e desempenho mesmo sob condições adversas.

3.7. Deverá implementar o serviço como DNS primário ou secundário, substituindo ou aumentando a infraestrutura DNS do TJCE.

3.8. A plataforma de DNS em nuvem deve prover:

3.8.1. Aceleração de resolução DNS;

3.8.2. Implementar DNSSEC (Domain Name System Security Extensions) com gerenciamento automático de chaves;

3.8.3. Implementar a configuração de até 320 de registros de DNS para funcionalidade de balanceamento de sites (Global Server Load Balancer – GSLB);

3.8.4. Proteção contra ataques direcionados aos serviços de DNS;

3.8.5. Implementar proteção contra os principais vetores de ataque a DNS, como por exemplo DNS Cache Poisoning, DNS Amplification, DNS Hijacking, DDoS, Domain Lookup e zero day;

3.8.6. Mecanismos que possibilitem a alta disponibilidade do serviço DNS;

Mecanismos para manutenção da configuração de DNS para os sites a serem protegidos;

3.8.7. Gráfico de volume por tipo de resposta de DNS ao longo do tempo.

3.9. A CONTRATADA deverá prover interface de gerenciamento dos serviços de DNS por meio de portal em nuvem e por meio de interfaces de programação de aplicação (APIs), permitindo integrações com ferramentas do TJCE.

Max Eduardo Vizcarra Melgar
Integrante Técnico

ANEXO III - TERMO DE NOMEAÇÃO DE PREPOSTO

Contrato ou Instrumento equivalente nº .....

Objeto da Demanda: .....

Por meio deste instrumento, a (nome da contratada) nomeia e constitui seu(sua) preposto(a), o(a) Sr.(a) (nome do/a preposto/a), inscrito(a) no Cadastro de Pessoas Físicas (CPF) sob o nº ....., para exercer a representação legal junto ao TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ - TJCE, com poderes para receber ofícios, representar a contratada em reuniões e assinar respectivas atas - obrigando a contratada nos termos dela constantes, debater, ajustar e receber solicitações e orientações para o cumprimento do contrato, notificações de descumprimento, de aplicação de penalidades, de rescisão, de convocação ou tomada de providências para ajustes e aditivos contratuais, e todas as demais que imponham, ou não, a abertura de processo administrativo ou prazo para a contratada responder, se defender ou tomar providências, e para representá-la em todos os demais atos que se relacionem à finalidade específica desta nomeação, que é a condução do contrato acima identificado.

Fortaleza, DIA de MÊS de ANO

.....
(nome da contratada)
(nome e assinatura do representante legal – confirmar poderes no estatuto social ou procuração)
(qualidade do representante legal – sócio-gerente, diretor, procurador)

.....
(nome e assinatura do/a preposto/a)

Documento assinado eletronicamente por **MAX EDUARDO VIZCARRA MELGAR**, **Gestor de Unidade**, em 02/06/2026, às 22:15, 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 **0733527** e o código CRC **EEE325B4**.

ANEXO IV - TERMO DE COMPROMISSO

O TRIBUNAL DE JUSTIÇA DO CEARÁ, sediado em Av. General Afonso Albuquerque Lima, S/N. – Cambeba, Fortaleza-CE CEP:60822-325 – Fone: (85) 3207-7000, CNPJ n° 09.444.530/0001-01, doravante denominado CONTRATANTE, e, de outro lado, a _____, sediada em _____, nº _____, _____, _____/__, CEP: __.___-___, CNPJ n° ___.___.___/____-__, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º __/20__ doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura

até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 156 da Lei nº. 14.133/21.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

O CONTRATANTE elege o foro de Fortaleza-CE, onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

DE ACORDO

CONTRATANTE	CONTRATADA

_____ Matrícula:	_____ Representante Legal
Testemunhas	
Testemunha 1	**Testemunha 2**
_____ Preposto da Contratada	_____ Fiscal Técnico

_____, _____ de _____ de 20____

Documento assinado eletronicamente por **MAX EDUARDO VIZCARRA MELGAR**, **Gestor de Unidade**, em 02/06/2026, às 22:18, 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 **0733529** e o código CRC **7B2EB1BE**.

Referência: Processo nº 8515550-95.2025.8.06.0000 SEI nº 0733529

ANEXO V - TERMO DE CIÊNCIA

INTRODUÇÃO
Visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos no projeto sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

IDENTIFICAÇÃO			
Contrato N°:			
Objeto:			
Contratante:			
Gestor do Contrato:		Matr.:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes no CONTRATANTE.

CIÊNCIA	
CONTRATADA – Funcionários	
_____ ***<Nome>*** **Matrícula: *<Matr.>***	_____ ***<Nome>*** **Matrícula: *<Matr.>***
_____ ***<Nome>*** **Matrícula: *<Matr.>***	_____ ***<Nome>*** **Matrícula: *<Matr.>***
_____ ***<Nome>*** **Matrícula: *<Matr.>***	_____ ***<Nome>*** **Matrícula: *<Matr.>***

_____,_____ de _____ de 20_____.

Documento assinado eletronicamente por **MAX EDUARDO VIZCARRA MELGAR**, **Gestor de Unidade**, em 02/06/2026, às 22:24, 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 **0733531** e o código CRC **31422D44**.

Referência: Processo nº 8515550-95.2025.8.06.0000 SEI nº 0733531

ANEXO VI - INSTRUMENTOS DE MEDIÇÃO DE RESULTADO (IMR)

1. DISPOSIÇÕES GERAIS

1.1. A avaliação da execução contratual será realizada por meio do Instrumento de Medição de Resultado (IMR), com base no cumprimento dos prazos e condições definidos neste Anexo.

1.2. Os Níveis Mínimos de Serviço (NMS) têm por finalidade estabelecer critérios objetivos para a aferição do desempenho da Contratada na prestação dos serviços contratados, assim como assistência técnica e garantia de funcionamento da solução, equipamentos e softwares integrantes do objeto da contratação.

1.3. A apuração do desempenho da Contratada será realizada mensalmente, considerando o período de referência de cada fatura, com base nas informações constantes do Relatório de Serviços Prestados (RSP).

1.4. A aferição do desempenho da Contratada será realizada de forma integral, não amostral, sendo vedada a aplicação de critérios amostrais ou médias compensatórias, com base nos registros constantes do Relatório de Serviços Prestados (RSP), sob responsabilidade da fiscalização do contrato, admitida a análise de justificativas técnicas devidamente fundamentadas, sem prejuízo da aplicação dos descontos previstos neste Anexo.

2. DESEMPENHO MENSAL DA PRESTAÇÃO DE SERVIÇO

2.1. O desempenho mensal da prestação de serviço da solução será medido por meio do cumprimento dos tempos definidos para os chamados abertos pela equipe técnica do Tribunal de Justiça do Estado do Ceará, considerando o impacto operacional e a criticidade da solução afetada.

2.2. Considerando a criticidade da solução para a continuidade dos serviços institucionais, os prazos de atendimento e recuperação serão contados em regime ininterrupto (24x7x365), salvo disposição expressa em contrário.

3. TIPOS DE CHAMADOS

3.1. O nível de severidade do chamado será atribuído exclusivamente pela equipe técnica do Tribunal de Justiça do Estado do Ceará no momento da abertura do chamado, com base no impacto operacional e na criticidade do serviço ou solução afetados.

3.2. O nível de severidade do chamado poderá ser reclassificado a critério da Contratante, a qualquer tempo, durante o atendimento, sempre que identificada divergência entre a classificação inicial e o impacto efetivo observado na operação dos serviços.

Tabela 1 - Classificação dos chamados

Severidade	Descrição

1	Chamado de alta criticidade, caracterizado pela **INDISPONIBILIDADE** total do uso dos produtos (equipamentos e/ou softwares), falha em ativo de rede ou software que resulte em paralisação do serviço, com impacto a múltiplos usuários e/ou em operações críticas do Tribunal.
2	Chamado de baixa criticidade, caracterizado por indisponibilidade parcial, degradação relevante de **DESEMPENHO**, falha intermitente ou degradação de tempo de resposta, sem paralisação total do serviço.
3	Atendimento de chamado sem cômputo para fins de NMS, caracterizado por solução disponível, ocorrência de alarmes, dúvidas operacionais, solicitações de informação ou ajustes não críticos, cujo atendimento poderá ser realizado de forma agendada, sem impacto relevante na continuidade do serviço.

4. DEFINIÇÃO DO TEMPO DE RECUPERAÇÃO OPERACIONAL (TRO)

4.1. Considera-se Tempo de Recuperação Operacional (TRO) o intervalo de tempo compreendido entre a abertura do chamado pela equipe técnica do TJCE e a efetiva restauração da disponibilidade da solução, devidamente validada pela Contratante, independentemente do encerramento administrativo do chamado.

4.2. Os chamados que ultrapassarem o TRO e permanecerem abertos continuarão gerando tempo de indisponibilidade para fins de apuração dos NMS, sendo considerados em todas as apurações mensais subsequentes até o efetivo fechamento.

4.3. Para fins de apuração do TRO, serão desconsiderados os períodos em que a Contratada permanecer aguardando ações, informações, liberações de acesso, validações técnicas ou quaisquer providências sob responsabilidade exclusiva da Contratante, desde que tais períodos estejam devidamente registrados e justificados no Relatório de Serviços Prestados (RSP).

4.4. FORNECIMENTO DE PEÇA

4.4.1. Os chamados classificados como “aguardando peça” somente poderão ter o prazo de contagem do Tempo de Recuperação Operacional (TRO) suspenso quando, cumulativamente:

4.4.1.1. o item estiver coberto por contrato de suporte ou garantia vigente;

4.4.1.2. o prazo de fornecimento da peça estiver previamente definido em instrumento contratual ou documental equivalente; e

4.4.1.3. houver comprovação documental da solicitação formal da peça junto ao fabricante ou fornecedor autorizado.

4.4.2. A suspensão do TRO limita-se exclusivamente ao período compreendido entre a comprovação da solicitação da peça e a sua efetiva disponibilização para instalação.

4.5. DEFEITO DE SOFTWARE (“BUG”)

4.5.1. Nos casos em que o atraso na solução do chamado técnico decorra da ocorrência de defeito de software ou “bug” formalmente reconhecido pelo fabricante, com a devida identificação do respectivo “bug-id”, a Contratada poderá apresentar exposição de motivos tecnicamente fundamentada.

4.5.2. A exclusão ou o abatimento de tempo para fins de apuração do TRO não será automático, dependendo de aceite expresso da Contratante, após análise da justificativa apresentada.

4.6. A suspensão do TRO não afasta a caracterização de indisponibilidade do serviço ou da solução, quando existente, para fins de apuração dos Níveis Mínimos de Serviço (NMS), do Indicador de

Desconto (ID) e do Indicador de Reincidência de Desconto (IRD).

5. PRAZOS DO TEMPO DE RECUPERAÇÃO OPERACIONAL (TRO)

5.1. O Tempo de Recuperação Operacional (TRO) e o respectivo regime de contagem aplicáveis aos chamados técnicos estão consolidados na tabela a seguir, em função da severidade do chamado e do impacto operacional do serviço afetado.

Tabela 2 - Tempos máximos e regime de contagem

Severidade	Tempo de Recuperação Operacional (TRO)	Regime de contagem
1	Até 4 (quatro) horas*	Tempo corrido (24x7x365)
2	Até 24 (vinte e quatro) horas	Tempo corrido (24x7x365)
3	Prazo definido na abertura do chamado	Tempo útil, das 8h às 20h

5.2. Para fins de aplicação dos prazos especiais para solução de contorno, consideram-se críticos os componentes, serviços ou equipamentos expressamente definidos como essenciais à continuidade das operações institucionais no Termo de Referência ou instrumento contratual correspondente, de acordo com a natureza do objeto contratado:

5.2.1. a totalidade da solução contratada, nos contratos cujo objeto seja a prestação de serviços;

5.2.2. a funcionalidade essencial da solução ou equipamento fornecido, nos contratos cujo objeto envolva fornecimento de bens com suporte ou garantia.

5.3. A caracterização da indisponibilidade crítica e dos respectivos componentes afetados dessa contratação são expressamente definidas abaixo:

5.3.1. **Lote 1 –** Indisponibilidade do Serviço de WAF em SaaS, causando indisponibilidade das aplicações do TJCE para o público em geral;

5.3.2. **Lote 2 –** Indisponibilidade simultânea dos 2 equipamentos do cluster ADC.

5.4. Na hipótese de indisponibilidade dos itens listados acima, com impacto crítico nas operações, a solução de contorno deverá ser implementada em até **2 (duas) horas corridas,** e a solução definitiva em até 8 (oito) horas corridas.

5.5. Considera-se solução de contorno a medida temporária que restabeleça a operação do serviço, ainda que de forma parcial, até a implementação da solução definitiva.

5.6. O prazo definido para chamados de severidade 3 tem caráter exclusivamente operacional, não sendo considerado para fins de NMS, ID ou IRD.

6. REGRA DE APLICAÇÃO DE GLOSAS

6.1. O descumprimento dos Níveis Mínimos de Serviço (NMS), evidenciado pela ultrapassagem do Tempo de Recuperação Operacional (TRO), implicará a aplicação de descontos financeiros incidentes sobre o valor mensal do contrato, conforme a severidade do chamado e o tempo de indisponibilidade excedente.

Tabela 3 - Percentuais de Glosas Aplicáveis por Severidade

Severidade	Situação	Desconto aplicável
1	Atraso superior ao TRO	2% (dois por cento) sobre o valor mensal do contrato, por hora de atraso
2	Atraso superior ao TRO	1% (um por cento) sobre o valor mensal do contrato, por hora de atraso

3	Atendimento negociado	Não se aplica

7. INDICADORES DE GLOSAS

INDICADORES DE GLOSAS			
Indicador	**01: Indicador de Indisponibilidade (II)**	**02: Indicador de Desconto (ID)**	**03: Indicador de Reincidência de Desconto (IRD)**
Finalidade	Medir o tempo total de indisponibilidade do serviço ou solução ao longo do mês.	Refletir financeiramente o desempenho da Contratada, com base no cumprimento dos Níveis Mínimos de Serviço (NMS), dos Tempos de Recuperação Operacional (TRO) e do tempo de indisponibilidade apurado pelo II.	Estimular a melhoria contínua do processo de gestão da disponibilidade dos serviços, minimizando o risco de reincidência de desempenho insatisfatório.
Meta / Limite	Quanto menor o tempo de indisponibilidade mensal, melhor o desempenho.	100% dos chamados solucionados dentro do respectivo TRO, observado o limite máximo mensal de desconto.	IRD = 0 ou 1: aceitável. IRD = 2: reincidência relevante. IRD ≥ 3: reincidência crítica.
Instrumento de medição	Relatório de Serviços Prestados (RSP).		Histórico de apuração do ID.
Critério de Acompanhamento e Apuração	todos os minutos de indisponibilidade ocorridos no mês.	todos os chamados registrados e o tempo de indisponibilidade apurado pelo II.	os meses em que o ID atingiu o limite máximo mensal.
Periodicidade e período de apuração	Mensal, por período de faturamento, do mês em análise.	Mensal, por período de faturamento, do mês em análise.	Mensal, por meio de janela móvel de 6 (seis) meses (mês em análise + 5 anteriores).
Evento considerado	Minutos em que o serviço permaneceu indisponível, total ou parcialmente, no mês.	a) Chamado técnico que ultrapassar o TRO, conforme severidade atribuída; e b) tempo total de indisponibilidade do serviço no mês, apurado pelo II.	Mês em que o ID atingir o limite máximo mensal de 30% do valor mensal do contrato.
Fórmula de cálculo	**II = soma dos minutos de indisponibilidade**	**ID (%) = mínimo entre 30 e (0,02 × TICSA + 0,01 × TICSB + 0,35 × II)**	**IRD = número de meses em que o ID atingiu o limite máximo mensal**
Definições e siglas	tempo total de indisponibilidade do serviço ou solução, em minutos, no mês, quando aplicável.	TICSA: tempo de indisponibilidade, em horas, excedente ao TRO, relativo a chamados de severidade 1. TICSB: tempo de indisponibilidade, em horas, excedente ao TRO, relativo a chamados de severidade 2. TRO: Tempo de Recuperação Operacional.	Ocorrência: mês em que o ID atinge o limite máximo mensal de 30%, no período de apuração.
Base de cálculo	Minutos totais de indisponibilidade no mês.	Valor mensal do contrato.	Histórico mensal do ID.

Impacto financeiro / Medidas	Não gera desconto isolado ou autônomo, sendo considerado exclusivamente como insumo para o cálculo do ID.	• Severidade 1: 2% do valor mensal do contrato por hora de atraso. • Severidade 2: 1% do valor mensal do contrato por hora de atraso • Indisponibilidade mensal: aplicação de peso de 0,35 por minuto, conforme fórmula do ID. • Desconto total limitado a 30 % do valor mensal do contrato. • Desconto contratual por desempenho operacional, aplicado diretamente no faturamento mensal.	• IRD = 0 ou 1: sem medidas adicionais. • IRD = 2: exigência de Plano de Ação Corretiva (PAC). • IRD ≥ 3: caracteriza desempenho crítico, resultando na aplicação das sanções administrativas previstas no contrato.
Fluxo de apuração	Registro da indisponibilidade → consolidação mensal → apuração do II.	Registro do chamado e da indisponibilidade → consolidação mensal → cálculo do ID → aplicação do desconto.	Consolidação histórica do ID → verificação do nível de reincidência → PAC → aplicação da multa correspondente.
Início de vigência	A partir da data de assinatura do contrato		
Observações	• O tempo de indisponibilidade deverá ser comprovado por registros técnicos e logs auditáveis. • Quando o Indicador de Indisponibilidade (II) não se aplicar ao objeto contratado, seu valor será considerado igual a zero (0) para fins de cálculo do ID.	• Chamados de severidade 3 não são considerados para fins de apuração dos NMS. • Suspensão do TRO somente nos termos contratuais. • O ID não se confunde com sanções administrativas.	• O Plano de Ação Corretiva (PAC) não afasta nem substitui a aplicação de sanções administrativas previstas em lei e no contrato.

8. DOS INDICADORES DE DESEMPENHO, GLOSA E REINCIDÊNCIA

8.1. O Indicador de Desconto (ID) será apurado mensalmente, nos termos definidos na Tabela de Indicadores constante deste Anexo, com base no cumprimento dos Níveis Mínimos de Serviço (NMS) e dos Tempos de Recuperação Operacional (TRO), observados os percentuais de desconto por severidade e o limite máximo mensal de 30% (trinta por cento) do valor mensal do contrato

8.2. A eventual tolerância operacional, negociação informal ou aceite tácito por parte da fiscalização não afasta a apuração objetiva dos Níveis Mínimos de Serviço nem a aplicação dos descontos previstos neste Anexo.

8.3. Para fins de apuração do Indicador de Reincidência de Desempenho (IRD), será considerada ocorrência cada mês em que o Indicador de Desconto (ID) atingir o limite máximo mensal de 30% (trinta por cento) do valor mensal do contrato.

8.4. O Indicador de Reincidência de Desempenho (IRD) corresponde ao número de ocorrências verificadas dentro do período de apuração, observado o limite de tolerância de, no máximo, duas ocorrências no período considerado, conforme definido na Tabela de Indicadores deste Anexo.

8.5. O IRD igual a 0 (zero) ou 1 (uma) ocorrência não enseja a adoção de medidas adicionais, mantendo-se o acompanhamento regular do desempenho contratual.

8.6. O IRD igual a 2 (duas) ocorrências implicará a exigência de apresentação de Plano de Ação Corretiva (PAC), a ser elaborado e apresentado pela Contratada no prazo definido pela fiscalização

do contrato.

8.7. O IRD igual ou superior a 3 (três) ocorrências caracterizará reincidência crítica, ensejando a aplicação da multa prevista no contrato, sem prejuízo da adoção de outras sanções administrativas cabíveis.

8.8. O Plano de Ação Corretiva (PAC) deverá conter, no mínimo, análise de causa raiz, medidas corretivas e preventivas, prazos de implementação e responsáveis pela execução.

8.9. A exigência de Plano de Ação Corretiva (PAC) não afasta nem substitui a aplicação das sanções administrativas cabíveis, inclusive multas, nos termos da legislação vigente, do instrumento contratual e da cláusula específica de sanções.

9. RELATÓRIO DE SERVIÇOS PRESTADOS (RSP)

9.1. O Relatório de Serviços Prestados deverá ser apresentado mensalmente, até o 5º (quinto) dia útil do mês subsequente, em formato eletrônico de planilha (.xls).

9.2. O sistema de controle de chamados adotado pela Contratada constitui a fonte oficial e única para fins de apuração do TRO, dos NMS, do ID e do IRD, prevalecendo seus registros sobre quaisquer outros meios de comunicação

9.3. O RSP deverá conter, no mínimo, as seguintes informações:

Tabela 6 - Estrutura Mínima do Relatório de Serviços Prestados (RSP)

Relatório de Serviços Prestados (RSP)	
Campo	**Descrição**
Data e hora de abertura do chamado	Registro inicial
Data e hora de início do atendimento	Início efetivo da atuação técnica da Contratada
Data e hora de conclusão	Encerramento
Número do ticket	Identificação do chamado
Severidade	Classificação
Elemento da solução	Serviço, Equipamento ou software
Descrição do problema	Identificação da falha
Providências adotadas	Diagnóstico realizado, solução de contorno (quando aplicável) e solução definitiva
Técnico solicitante	Equipe técnica do TJCE
Técnico executor	Responsável da Contratada
Períodos suspensos do TRO	Intervalos desconsiderados por responsabilidade da Contratante
TRO contratual	Prazo máximo de recuperação aplicável ao chamado
TRO apurado	Tempo efetivamente apurado para fins de NMS
Tempo excedente ao TRO (horas)	Tempo de indisponibilidade excedente ao TRO, considerado para fins de cálculo do ID
Resultado para fins de NMS	Cumprido / Descumprido
Justificativa técnica	Fundamentação para eventuais atrasos ou suspensões
II	tempo total de indisponibilidade do serviço ou solução, em minutos, no mês, quando aplicável

ID	Desconto aplicado percentual ou valor do indicador de desconto
IRD	Valor acumulado do Indicador de reincidência de desconto no período de 6 (seis) meses

9.4. Na inexistência de chamados técnicos no mês de apuração, e desde que comprovado o cumprimento integral das obrigações contratuais, o pagamento mensal será efetuado integralmente.

9.5. Cada chamado técnico será avaliado de forma individual, sendo vedada a compensação de desempenho entre chamados, ainda que ocorram no mesmo período de apuração.

9.6. A apuração dos NMS e a aplicação dos descontos independem do fechamento do chamado, sendo realizadas mensalmente com base nas informações constantes do RSP.

9.7. RELATÓRIO DE ANÁLISE DE CAUSA RAIZ (RCA)

9.7.1. Para todos os chamados classificados como Severidade 1, a Contratada deverá apresentar Relatório de Análise de Causa Raiz (RCA) como anexo do Relatório de Serviços Prestados (RSP) do período de apuração correspondente, sendo a entrega do RCA vinculada ao prazo de apresentação do respectivo RSP

9.7.2. O Relatório de Análise de Causa Raiz (RCA) deverá observar, no mínimo, a seguinte estrutura, contexto técnico do evento, sem repetição integral das informações já registradas no Relatório de Serviços Prestados (RSP):

9.7.2.1. Identificação do incidente;

9.7.2.2. Descrição resumida do incidente;

9.7.2.3. Análise da causa raiz – descrição objetiva da causa principal identificada e dos fatores contribuintes relevantes;

9.7.2.4. Lições aprendidas;

9.7.2.5. Ações corretivas e preventivas.

9.7.3. A não apresentação do RCA juntamente com o RSP, ou a sua apresentação de forma incompleta ou inconsistente, será considerada descumprimento de obrigação contratual, passível da adoção das medidas administrativas cabíveis, sem prejuízo dos descontos já aplicados por descumprimento dos Níveis Mínimos de Serviço (NMS).

Documento assinado eletronicamente por **MAX EDUARDO VIZCARRA MELGAR**, **Gestor de Unidade**, em 02/06/2026, às 22:42, 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 **MATHEUS FREIRE E SILVA DO NASCIMENTO**, **Gestor de Unidade**, em 16/07/2026, às 15:57, 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**, **Servidor**, em 17/07/2026, às 09:36, conforme horário oficial de Brasília, com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015.

ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

TERMO DE RECEBIMENTO DEFINITIVO

Nº	XXXX		
OBJETO DA DEMANDA	XXXX		
FORNECEDORA	XXX	**CNPJ**	XXX
Nº DA OS/OF	XXX		
DATA DA EMISSÃO	XXX		

Por este instrumento, fica registrado que os itens recebidos provisoriamente na data de XX/XX/XXXX correspondentes ao contrato ou à ordem de serviços acima identificada(o) atendem às condições contratuais, de acordo com os critérios estabelecidos no Termo de Referência.

De acordo com os critérios de aceitação e demais termos contratuais, não há incidência de descontos por desatendimento dos Instrumentos de Medição de Resultados.

Não foram OU Foram identificadas inconformidades que ensejam glosas, merecendo aplicação do XXXXX a ser considerado no próximo XXXX, e sanções, que reclamada a instrução em processo administrativo próprio.

Pelo analisado, o valor a liquidar correspondente ao recebimento ora confirmado é de R$ XXX (XXX).

Local, Data

_____

NOME DO REPRESENTANTE DO TJCE- FISCAL

Matrícula: xxxxxx

Caso a movimentação dos itens tenha se dado apenas por nota de simples remessa, AUTORIZA-SE a **FORNECEDORA** apresentar as notas fiscais dos itens ora recebidos em definitivo no valor bruto de R$ XXX (XXX), merecendo ainda os destaques fiscais impostos.

_____

NOME DO REPRESENTANTE DO TJCE- GESTOR

Matrícula: xxxxxx

Documento assinado eletronicamente por **MAX EDUARDO VIZCARRA MELGAR**, **Gestor de Unidade**, em 02/06/2026, às 23:25, 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 **0733534** e o código CRC **27D3736B**.

Referência: Processo nº 8515550-95.2025.8.06.0000 SEI nº 0733534

ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

TERMO DE RECEBIMENTO PROVISÓRIO

O Nº	XXXX		
OBJETO DA DEMANDA	XXXX		
FORNECEDORA	XXX	**CNPJ**	XXX
Nº DA OS/OF	XXX		
DATA DA EMISSÃO	XXX		

Por este instrumento, fica registrado que foram recebidos provisoriamente na presente data e serão objeto de avaliação técnica quanto à adequação da entrega:

- XXXXX;

- XXXXX.

Ressaltamos que o recebimento definitivo para ateste de recebimento ocorrerá somente após a verificação e confirmação de atendimento dos requisitos e demais condições contratuais, especialmente as especificações constantes do Termo de Referência relacionado ao Contrato acima identificado.

Local, Data.

_____

NOME DO REPRESENTANTE DO TJCE

Matrícula: xxxxxx

Documento assinado eletronicamente por **MAX EDUARDO VIZCARRA MELGAR**, **Gestor de Unidade**, em 02/06/2026, às 23:27, 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 **0733535** e o código CRC **F59EDA8F**.

Referência: Processo nº 8515550-95.2025.8.06.0000 SEI nº 0733535

ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
COORDENADORIA DE CIBERSEGURANÇA

MAPA DE PREÇOS

CÓDIGO PAC 2026: RDP-SETIN-2026-26

AQSETIN2025003 – Solução de balanceamento de carga e WAF

1. INTRODUÇÃO

Este documento tem como finalidade apresentar o valor estimado da contratação, como também a memória de cálculo e as fontes de preços utilizadas.

2. DESCRIÇÃO DOS SERVIÇOS E QUANTITATIVO

2.1. A tabela a seguir apresenta a consolidação dos serviços e respectivos quantitativos extraídos do ANEXO I – Especificações Técnicas

LOTE 1			
Id	**Bem/Serviço**	**UND**	**Qtd.**
1	Solução ADC	**UND**	**2**
2	Suporte	**MÊS**	**57**
3	Treinamento	**ALUNO**	**8**
4	Instalação	**UND**	**2**

LOTE 2			
Id	**Bem/Serviço**	**UND**	**Qtd.**
1	Web Application Firewall (WAF) em modelo Software como Serviço (SaaS), com franquia mensal de 50 TB de tráfego inspecionado.	**Mês**	**36**
2	Franquia adicional de tráfego inspecionado a ser consumido e contratado sob demanda durante a vigência contratual	**TB**	**900**
3	Proteção DNS para 1 zona	**Mês**	**36**

3. FONTES UTILIZADAS NA PESQUISA DE MERCADO

3.1. A pesquisa de preços para a presente contratação foi realizada em conformidade com as diretrizes estabelecidas no Manual de Pesquisa de Preços do TJCE, Capítulo II, Seção I, art. 4º, incisos I e II. Para a definição do valor estimado da contratação, foram consideradas as seguintes fontes de informação:

3.2.1. Preços adjudicados e atas de registro de preços publicados no Portal de Compras do Estado do Ceará, bem como valores constantes nos sistemas oficiais do Governo Federal, incluindo o painel de consultas disponível no Portal Nacional de Contratações Públicas (PNCP);

3.2.1. Contratações similares realizadas pela Administração Pública, em execução ou concluídas no período de até 1 (um) ano anterior à data da pesquisa de preços, inclusive por meio de sistema de registro de preços, observada a atualização dos valores pelos índices correspondentes.

3.2. Pesquisa direta com fornecedores

3.2.1. De acordo com o Manual de Pesquisa de Preços do TJCE, Capítulo II, Seção I, §2º, a pesquisa de preços por meio da modalidade prevista no inciso IV (pesquisa direta com, no mínimo, 3 fornecedores) deve ser evitada sempre que possível.

3.2.2. Considerando essa orientação, não foi realizada pesquisa direta com fornecedores para a presente contratação. Foram utilizadas outras fontes de pesquisa disponíveis, as quais se mostraram suficientes para a definição do valor estimado.

3.3. Contratações similares feitas pela Administração Pública:

3.3.1. A seguir, apresenta-se a tabela consolidada das contratações identificadas, contemplando informações relativas ao órgão contratante, instrumento contratual, período de vigência e descrição do objeto.

Lote	Órgão/ Entidade	Contrato/ Ata	Vigência	Objeto	URL
1	**TJRO**	Ata nº 00004/2025 Contratos nº 53/2025 e 23/2026	06/03/2025 a 05/03/2026	Solução de balanceamento de aplicação	https://pncp.gov.br/app/atas/04293700000172/2025/15/1 https://pncp.gov.br/app/contratos/04293700000172/2025/173 https://pncp.gov.br/app/contratos/04293700000172/2026/15
	STJ	Contrato nº 108/2023	11/12/2023 a 11/12/2028	Fornecimento de solução de Web Application Firewall (WAF)	https://pncp.gov.br/app/contratos/00488478000102/2023/171
	TRF 1	Contrato nº 00014/2024	18/03/2024 a 05/08/2029	Solução de balanceadores de carga	https://pncp.gov.br/app/contratos/00508903000188/2024/1352
	TRF3 (CJF)	Ata nº 008/2025 (CJF) Contrato nº 0700610/2025	15/12/2025 a 15/03/2031	Solução tecnológica de Controlador de Entrega de Aplicações (ADC)	https://pncp.gov.br/app/atas/00508903000188/2025/1742/1 https://pncp.gov.br/app/contratos/59949362000176/2025/246
	TRT 4	Contrato nº 52/2022	04/08/2022 a 01/06/2026	(SETIC-62/2022) Solução de proteção de borda de rede e de alta disponibilidade (Registro de Preços).	https://silc.trt4.jus.br/#/publico/contratos

Lote	Órgão/ Entidade	Contrato/ Ata	Vigência	Objeto	URL
2	**SERPRO**	Contrato nº 197887	24/08/2024 a 23/08/2027	Contratação por consumo de USN (Unidade de Serviços em Nuvem) de Plataforma de Segurança em Nuvem para Tratamento e Proteção de Sítios Web com CDN (Content Delivery Network)	https://www.transparencia.serpro.gov.br/@@contratos https://lowcode.serpro.gov.br/Contratos/rest/api/ArquivoContrato?nome_arquivo=siga_197887.pdf&id_arquivo=123466
	TJRN	Contrato nº 76/2021	203/01/2022 a 03/07/2027	Fornecimento e suporte de solução de Controle de Acesso à Rede (Network Access Control – NAC) e Firewall de Aplicação Web (Web Application Firewall – WAF)	https://tjrn.jus.br/documentos/contratos-vigentes/226-contrato-n-762021/
	TRF3	Contrato nº 04.042.10/2024	30/12/2024 a 09/04/2030	Solução de alta disponibilidade e proteção dos ativos de negócio	https://pncp.gov.br/app/contratos/59949362000176/2024/211

4. MEMÓRIA DE CÁLCULO

4.1. Com base nos valores obtidos na pesquisa de mercado apresentada na Seção 3, foi elaborada a memória de cálculo do valor estimado da contratação, mediante aplicação de análise estatística sobre os preços coletados, com o objetivo de avaliar a dispersão dos dados e definir o critério mais adequado para determinação do valor de referência.

4.2. Metodologia estatística aplicada à análise dos preços

4.2.1. Após a coleta dos valores unitários, foi realizada análise estatística da amostra, com o objetivo de avaliar a consistência dos dados coletados e verificar o grau de dispersão dos preços identificados na pesquisa de mercado.

4.2.2. Inicialmente foi calculada a **média simples** dos valores obtidos na pesquisa de preços. Em seguida, foi apurado o **coeficiente de variação (CV)**, indicador estatístico que mede o grau de dispersão dos dados em relação à média da amostra.

4.2.3. Conforme orientações constantes no capítulo *"Definição e Execução da Forma de Cálculo do Valor Estimado da Contratação"* do **Manual de Licitações e Contratos – Orientações e Jurisprudência do TCU** (5ª edição, versão 3.0, p. 359), o coeficiente de variação pode ser utilizado como parâmetro para avaliar a homogeneidade dos preços coletados e auxiliar na definição do método de cálculo do valor de referência (**média ou mediana**).

4.2.4. O coeficiente de variação é considerado baixo quando apresentar percentual **igual ou inferior a 25%**, situação em que os dados são considerados homogêneos e a **média** pode ser utilizada como critério de definição do valor de mercado.

4.2.5. Nos casos em que o coeficiente de variação seja **superior a esse limite**, indicando maior dispersão dos valores coletados, recomenda-se a utilização da **mediana**, por ser uma medida estatística menos sensível à influência de valores extremos.

4.3. Aplicação da metodologia e análise dos resultados

4.3.1. Aplicada a metodologia descrita no item anterior, foram calculados os indicadores estatísticos da amostra de preços coletados para cada item da contratação, incluindo mediana, média simples, desvio padrão e coeficiente de variação.

4.3.2. Os resultados obtidos encontram-se apresentados nas tabelas de análise estatística a seguir, nas quais é possível verificar os valores considerados na pesquisa de preços e os respectivos indicadores estatísticos.

4.3.3. A partir do cálculo do **coeficiente de variação (CV)** para cada item analisado, foi possível avaliar o grau de dispersão dos preços coletados na pesquisa de mercado. Com base nos parâmetros descritos no item **4.2**, foi adotada a **média** para os itens que apresentaram coeficiente de variação **igual ou inferior a 25%** e a **mediana** para aqueles cujo coeficiente de variação **superou esse limite**.

4.3.4. Dessa forma, o critério estatístico foi aplicado individualmente a cada item analisado adotando-se média ou mediana conforme o comportamento da amostra de preços. Os resultados obtidos encontram-se demonstrados nas tabelas de análise estatística referentes aos **Lotes 1 e 2**, e os valores finais considerados para a composição do orçamento estimado estão consolidados na **Seção 5 – Custo Total Estimado**.

4.4. Durante a pesquisa de mercado foram identificadas diversas licitações com objetos semelhantes ao pretendido pelo TJCE. Observou-se que parte significativa desses certames foi vencida por cloud brokers, que ofertam soluções baseadas em diferentes provedores de infraestrutura e serviços de proteção de aplicações web. Considerando essa característica do mercado, foram selecionadas como referência as licitações cujas características técnicas, modelo de contratação e perfil de consumo apresentavam maior aderência ao objeto desta contratação, ainda que vinculadas a um mesmo provedor de tecnologia. Essa seleção buscou garantir que os valores utilizados na formação do preço estimado refletissem condições reais de contratação de soluções equivalentes, preservando a representatividade da amostra analisada.

4.5. Foi dada prioridade às licitações cuja franquia base de tráfego contratada era próxima da franquia pretendida pelo TJCE. A motivação foi obter um preço compatível com o perfil de consumo exigido pelo órgão, em vez de formar uma média com muitas cotas de franquia adicional que não representariam adequadamente a realidade operacional do serviço. O consumo muito acima da franquia base do provedor não são sustentáveis e distorceriam o custo estimado; por isso, licitações com franquia base mais alta foram priorizadas na composição da média.

4.6. Na presente contratação, a solução foi estruturada em dois lotes distintos: Lote 1 – ADC on-premises e Lote 2 – WAF como serviço em nuvem. Contudo, durante a pesquisa de mercado verificou-se que, em diversas licitações analisadas, as soluções de Application Delivery Controller (ADC) e Web Application Firewall (WAF) são contratadas de forma conjunta em ambientes on-premises, sendo disponibilizadas em um mesmo equipamento físico e diferenciadas principalmente pelos módulos de licenciamento habilitados. Nesses casos, o valor apresentado nos certames normalmente contempla hardware, licenciamento de ADC e licenciamento de WAF, agregados em um único item ou lote.

4.7. Essa característica das contratações analisadas gerou distorção na comparação direta dos preços, uma vez que o Lote 1 do TJCE contempla apenas a funcionalidade de ADC, enquanto parte das referências de mercado incluía também o licenciamento adicional de WAF. Para adequar os valores ao escopo efetivamente contratado, foi realizado ajuste nos preços obtidos nas licitações que apresentavam ADC + WAF on-premises. O redutor aplicado, de 18% (dezoito por cento), foi identificado a partir da análise detalhada do edital do TJRO, no qual os módulos de licenciamento da solução estão discriminados. A partir dessa informação, foram somados os valores correspondentes aos licenciamentos de WAF e verificado o impacto percentual desses componentes em relação ao valor total da contratação, permitindo estimar a participação do WAF no custo global da solução. Com base nesse percentual, procedeu-se ao ajuste dos valores utilizados na pesquisa de mercado, de forma a considerar apenas os custos compatíveis com o escopo do Lote 1 (ADC), evitando a incorporação de funcionalidades não previstas na contratação e assegurando maior aderência entre o valor estimado e o objeto licitado.

TJRO - Ata nº 00004/2025			
Item	**Valor**	**Percentual (%)**	**Funcionalidade**
1 – Hardware R4800 (ADC/WAF)	R$ 1.800.000	**78%**	Equipamento físico onde roda ADC, WAF etc.
2 – Big-IQ	R$ 80.000	**3%**	Licença para Gestão centralizada do equipamento (configuração, políticas, backups).

3 – IP Intelligence	R$ 120.000	**5%**	Licença para Reputação IP, bloqueio de botnets, TOR, scanners (usado no WAF).
4 – Threat Campaigns (WAF)	R$ 305.000	**13%**	Licença para Assinaturas avançadas de ataques web e APIs (exclusivo do WAF).
Total	**R$ 2.305.000**	**100%**	Soma geral dos itens avaliados.

4.8. MEMÓRIA DE CÁLCULO - LOTE 1

4.8.1. Item 1 – Solução ADC

4.8.1.1. Para composição do valor do Item 1, foram analisadas referências de contratações públicas equivalentes, todas envolvendo soluções de Application Delivery Controller (ADC) e Web Application Firewall (WAF) sobre o mesmo appliance físico, com licenciamento variável. Quando necessário, aplicou-se redutor de 18% exclusivamente sobre a parcela de hardware/software para exclusão do licenciamento WAF não contemplado no escopo do TJCE.

4.8.1.2. Tribunal de Justiça do Estado de Rondônia (TJRO), Ata de Registro de Preços 00004/2025

GRUPO	ITEM	ESPECIFICAÇÕES	QUANTIDADE	UNIDADE	VALOR UNITÁRIO DO ITEM (R$)	VALOR TOTAL DO ITEM (R$)
1	1	Renovação das licenças e upgrade de hardware para a solução de balanceamento utilizado no TJRO Marca: F5 Networks Modelo: R4800	2	unidades	900.000,00	1.800.000,00
	2	Renovação do suporte Big IQ Marca: F5 Networks Modelo: Big IQ	1	unidade	80.000,00	80.000,00
	3	Renovação do suporte IP Intelligence Marca: F5 Networks Modelo: IP Intelligence	1	unidade	120.000,00	120.000,00
	4	Renovação do suporte Threat Campaign Marca: F5 Networks Modelo: Threat Campaign	1	unidade	305.000,00	305.000,00
	5	Serviço de Operação Assistida e Monitoramento Especializado – 36 meses	1	unidade	432.000,00	432.000,00
	6	Vouchers de Treinamento 1: F5 ADM Big IP – Administering Big IP	6	unidades	6.500,00	39.000,00
	7	Vouchers de Treinamento 2: F5 LTM – Configuring Big IP Local Traffic Manager	6	unidades	6.500,00	39.000,00

Item do Contrato	Descrição	Cálculo	Valor (R$)
Grupo 1 – Item 1	F5 R4800	—	**900.000,00**
Grupo 1 – Item 2	Renovação do Suporte Big-IQ	—	**80.000,00**
—	**Total**	—	**980.000,00**

4.8.1.3. Superior Tribunal de Justiça (STJ), Contrato nº 108/2023

CLÁUSULA QUARTA - DO PREÇO E DO VALOR DO CONTRATO

4.1 O preço dos itens e o valor do Contrato STJ n. 108/2023, a partir de 14/11/2024, ficam definidos conforme planilha abaixo discriminada:

Item	Especificação do Objeto	Marca/ Modelo	Unidade	Qtde.	Preço Unitário	Preço Total
1	SERVIDOR/STORAGE Fornecimento de Solução de Web Application Firewall - WAF.	F5/r4800	Unid.	2	R$ 1.165.188,50	R$ 2.330.377,00
2	INSTALAÇÃO DE EQUIPAMENTOS DE TI Instalação e Configuração.	Serviço Teltec	Unid.	2	R$ 65.750,00	R$ 131.500,00
3	SUPORTE DE INFRAESTRUTURA DA TI	Serviço Teltec	Mensal	11	R$ 4.790,00	R$ 52.690,00

				49	R$ 5.119,55	R$ 250.858,05
4	TREINAMENTO/CAPACITAÇÃO EM TIC	Serviço Teltec F5	Pessoa	4	R$ 24.950,00	R$ 99.800,00
VALOR TOTAL DO CONTRATO						**R$ 2.865.225,05**

4.2 O valor *pro rata* do Contrato STJ n. 108/2023, para o período de 11/12/2023 a 11/12/2028, fica estabelecido em R$ 2.865.225,05 (dois milhões, oitocentos e sessenta e cinco mil, duzentos e vinte e cinco reais e cinco centavos).

Item do Contrato	Descrição	Cálculo	Valor (R$)
Item 1	Solução WAF	1.165.188,50	—
—	Redutor 18%	1.165.188,50 × 0,82	**955.454,57**
—	**Total**	—	**955.454,57**

4.8.1.4. Tribunal Regional Federal da 3ª Região (TRF3), Contrato nº 0700610/2025, da Ata nº 008/2025 do Conselho da Justiça Federal (CJF)

CLÁUSULA NONA – DO VALOR DO CONTRATO

9.1 O valor total contratado fica estimado em **R$ 9.388.000,00 (nove milhões e trezentos e oitenta e oito mil reais)**, referente ao Grupo 1 do Edital PE nº 90.008/2025, conforme especificado a seguir:

GRUPO	ITEM	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE		VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
				TRF 3	JFPG/SP		
1	1.1	Appliance físico para solução de Application Delivery Controller – ADC, fabricante F5, Modelo BIG-IP R4800	unidade	2	2	1.790.000,00	7.160.000,00
	1.2	Serviço de instalação e configuração da solução ADC	unidade	2	2	88.000,00	352.000,00
	1.3	Serviço de garantia e suporte técnico presencial para a solução ADC	mês	60	60	13.000,00	1.560.000,00
	1.4	Transferência de conhecimento online, com carga horária mínima de 40h	pessoa	10	0	25.000,00	250.000,00
	1.5	Serviços técnicos especializados para implementação e customização da solução ADC	hora	120	120	275,00	66.000,00
VALOR TOTAL DA CONTRATAÇÃO (R$)							**9.388.000,00**

Item do Contrato	Descrição	Cálculo	Valor (R$)
Grupo 1 - Item 1.1	R4800	1.790.000,00	—
—	Redutor 18%	1.790.000,00 × 0,82	**1.467.800,00**
—	**Total**	—	**1.467.800,00**

4.8.1.5. Tribunal Regional Federal da 1ª Região (TRF1), Contrato nº 00014/2024

ANEXO III AO CONTRATO N. 0014/2024
PLANILHA DE PREÇOS (R$)

Item	Descrição	Und.	Qtd.	Valor Unitário	Valor Total
1	**Solução de Balanceador de Carga com garantia de 60(sessenta) meses.** **Fabricante**: A10 Networks **Modelo**: Thunder 5440S CFW, 1U, 1Xcpu, 4X40GF, 24x10GF, 64GB, SSD, LOM, 2xFTA/FPGA, S+R ASIC, Dual Chip H/W SSL, Railtik, (Dual N1 SSL Gen 3 Card), H/W Only **PART NUMBER HW**: TH5440-010-N1SSL2-CFW-H **PART NUMBER SW**: TH5440-010-N1SSL2-CFW-S Suporte/Garantia por 60 Meses	Und.	2	1.245.900,00	2.491.800,00
2	Serviço de Instalação, Implantação e Integração dos Produtos	serviço	1	40.000,00	40.000,00
3	Operação assistida	serviço	1	6.000,00	6.000,00
4	Treinamento	Turma	2	38.200,00	76.400,00
Valor Total					**2.614.200,00**

Item do Contrato	Descrição	Cálculo	Valor (R$)
Item 1	Solução de Balanceador	1.245.900,00	—
—	Redutor 18%	1.245.900,00 × 0,82	**1.021.638,00**
—	**Total**	—	**1.021.638,00**

4.8.1.6. Lote 1, Item 1 (ADC)

Fonte	Total considerado (R$)
TJRO	**980.000,00**
STJ	**955.454,57**
TRF3/CJF	**1.467.800,00**
TRF1	**1.021.638,00**

4.8.2. Item 2 – Suporte Técnico

Fonte	Item do Contrato	Descrição	Cálculo	Valor mensal (R$)
TJRO	Grupo 1 – Item 5	Serviço de Operação por 36 meses	432.000 ÷ 36*	**12.000,00**
STJ	Item 3	Suporte	—	**5.119,55****
TRF3/CJF	Item 1.3 do Grupo 1	Serviço de garantia e Suporte	—	**13.000,00**

*TJRO – valor total unitário total do contrato dividido pela vigência para encontrar o valor mensal.

**STJ – O item de suporte do contrato do STJ sofreu reajuste de R$4.790,00 para R$5.119,55, conforme apresentado na figura acima, no item 4.8.1.3.

4.8.3. Item 3 – Treinamentos

Fonte	Item do Contrato	Descrição	Unidade	Cálculo	Valor (R$)
TJRO	Grupo 1 - Itens 6 e 7	Treinamento 1 Treinamento 2	Voucher/Pessoa	6.500 + 6.500	**13.000,00**
STJ	Item 4	Treinamento/Capacitação	Pessoa	—	**24.950,00**
TRF1	Item 4	Treinamento	Turma de 4 pessoas, conforme documento RELAÇÃO DE ITENS - PREGÃO ELETRÔNICO Nº 00056/2023-000 (item 6.4.4.), presente na aba "Arquivos" deste link.	38.200 ÷ 4	**9.550,00**
TRF3/CJF	Item 1.4	Transferência de conhecimento	Pessoa	—	**25.000,00**

4.8.4. Item 4 – instalação

Fonte	Item do Contrato	Descrição	Cálculo	Valor (R$)
STJ	Item 2	Instalação	—	**66.750,00**
TRF3/CJF	Grupo 1 - Item 1.2	Instalação	—	**88.000,00**
TRF1	Item 2	Instalação	—	**40.000,00**

4.9. MEMÓRIA DE CÁLCULO – LOTE 2

4.9.1.TRT-4, Contrato nº 52/2022

Item da Ata	Descrição	Unid.	Quant.	Preço Unitário (R$)	Preço Total (6 meses) (R$)	Preço mensal por item (R$)
2	**Prestação de serviços de proteção de borda de rede e de alta disponibilidade** através de rede dinâmica de distribuição e aceleração de conteúdo - CDN, integrada a recursos de segurança de firewall de aplicação web - WAF, mitigação contra ataques distribuídos de negação de serviço - DDoS, gerenciamento de robôs (botnets) incluindo suporte técnico, por **36 meses**, para um tráfego de até **40 TB mensais.**	**Serviço**	**1**	**1.005.022,52 (36 meses)**	**167.503,74**	**27.917,29**
4	**Franquia de tráfego adicional (TB)**	**TB**	**30**	**494,51**	**14.835,30**	**2.472,55**
5	**Proteção DNS**	**Zonas DNS**	**2**	**17.641,87 (36 meses)**	**5.880,60**	**980,10**

Item do Contrato	Descrição	Cálculo	Valor (R$)
Item 2	Proteção de borda 40 TB	27917,29 ÷ 40 TB = 697,93/TB	
—	Proporção de 50 TB para TJCE	697,93 × 50 TB*	**34.896,61**
Item 4	Franquia de tráfego adicional por TB	—	**494,51**
Item 5	Proteção DNS 2 Zonas*	**980,10**÷ 2**	**490,05**

* foi considerado apenas 1 TB para encontrar o valor unitário aplicado ao quantitativo de 50 TB estimado para o TJCE

** foi considerado apenas 1 zona de DNS para encontrar o valor unitário aplicado ao quantitativo estimado para o TJCE

4.9.2. TJRN, Contrato nº 76/2021

MEMÓRIA DE CÁLCULO DO REAJUSTE (ICTI/IPEA)			
VALOR GLOBAL DO CONTRATO	ÍNDICE DO PERÍODO	VALOR DO REAJUSTE	VALOR GLOBAL REAJUSTADO
1.355.148,00	6,96%	94.318,30	1.449.466,30

[redacted]

VALOR CONTRATUAL REAJUSTADO						
GRUPO	ITEM	DESCRIÇÃO	UNID	QUANT. PREVISTA	VALOR UNITÁRIO	VALOR TOTAL
1	1	Solução de Firewall de Aplicações WEB (WEBAPLICATION FIREWALL-WAF)	Mês	30	R$ 40.810,53	R$ 1.224.316,03
	2	Franquia adicional de tráfego para o item 1	Terabyte	60 *	R$ 1.648,96	R$ 98.937,57
	3	Proteção DNS para 3 zonas	Mês	30	R$ 4.207,09	R$ 126.212,70
VALOR TOTAL						R$ 1.449.466,30

* 60 TB para os 30 meses de contrato, sendo utilizados somente após expedida a franquia do item 1.

Item do Contrato	Descrição	Unidade	Cálculo	Valor (R$)
Grupo 1 Item 1	Solução de firewall de aplicações WEB	Mês	40.810,53*	**40.810,53**
Grupo 1 Item 2	Franquia adicional de tráfego para o item 1	Terabyte	—	**1.648,96**
Grupo 1 Item 1 + Item 3	Proteção DNS para 3 zonas*	Mês	4207,09 ÷ 3**	**1.402,36**

* Para o contrato do TJRN, não foi adotada a proporcional do valor com base no volume estimado de tráfego (TB), uma vez que o conforme 3º Termo Aditivo ao Contrato nº 76/2021 – TJRN, houve ampliação significativa da franquia mensal suportada (acréscimo de 41 TB, totalizando 65 TB/mês) sem qualquer impacto no valor mensal contratado, demonstrando que a formação de preços nesse contrato de serviço não segue relação linear entre volume de dados e custo. Assim, para fins de estimativa, adotou-se o valor global apresentado no contrato.

CLÁUSULA PRIMEIRA – DO OBJETO:

1.1. O presente Termo Aditivo tem por objeto a alteração quantitativa do Contrato nº 76/2021, a fim de acrescer no item 01 mais 41 TB, passando a Solução de Firewall de Aplicações WEB (WEB APLICATION FIREWALL – WAF) suportar até 65 TB por mês.

** foi considerado apenas 1 zona de DNS para encontrar o valor unitário aplicado ao quantitativo estimado para o TJCE

4.9.3. SERPRO, Contrato nº 197887

Grupo	Item	Descrição	Unidade	Quantidade 36 meses (Y)	Valor Unitário Mensal (R$) (A)	Valor Total 36 meses (R$) (YxA)
1	1	Plataforma de Proteção Básica e distribuição de conteúdo para proteção de sítios Web HTTP e HTTPS vinculadas a domínio DNS e seus respetivos subdomínios	USN1	1.700 Unidades de 1TB.	R$ 2.973,29	R$ 5.054.593,00
	2	Unidade de 1 TB de Proteção de TB adicional para USN1 pelo período de 1 mês	USN2	1.700 Unidades adicionais de 1 TB.	R$ 656,95	R$ 1.116.815,00
	3	Plataforma de Proteção Avançada e distribuição de conteúdo para proteção de sítios Web HTTP e HTTPS vinculadas a domínio DNS e seus respetivos subdomínios	USN3	2.000 Unidades de 3TB.	R$ 5.449,72	R$ 10.899.440,00
	4	Unidade adicional de 1 TB de Proteção para USN3 pelo período de 1 Mês	USN4	2.000 Unidades adicionais de 1 TB.	R$ 1.456,42	R$ 2.912.840,00

Item do Contrato	Descrição	Cálculo	Valor (R$)
Grupo 1 – Item 3	Proteção 3TB	5.449,72 ÷ 3* = 1.816,57 por TB	—
—	Proporção de 50 TB para TJCE	1.816,57 × 50 TB*	**90.828,67**
Grupo 1 – Item 4	Unidade adicional 1 TB	—	**1.456,42**

* foi considerado apenas 1 TB para encontrar o valor unitário aplicado ao quantitativo de 50 TB estimado para o TJCE

4.9.4. TRF-3, Contrato nº 04.042.10/2024

ITEM	ESPECIFICAÇÃO	PART NUMBER	UNIDADE DE MEDIDA	CATMAT CATSER	QTDE	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
1	Prestação de serviços de solução de alta disponibilidade e proteção dos ativos de negócio da JF3R através de rede dinâmica de distribuição e aceleração de conteúdo - CDN, integrada a recursos de segurança de firewall de aplicação web - WAF, mitigação contra ataques distribuídos de negação de serviço - DDoS, gerenciamento de robôs (*bomets*) incluindo suporte técnico e passagem de conhecimento, com tráfego de até 66TB mensais.	Akamai App & API Protector Included Delivery Akamai Bot Manager Premier Akamai Malware Protection	mês	27502	60	118.500,00	7.110.000,00
2	Franquia de tráfego adicional para o item 1 para 60 (sessenta) meses	-	Gigabytes	26077	420.000	1,30	546.000,00
3	Proteção DNS para 5 zonas	Akamai Edge DNS SEC 5 Zones Akamai Edge DNS 5 Zones	mês	26077	60	1.950,34	117.020,40

4	Serviços de instalação e ativação da solução	-	serviço	27120	1	30.000,00	30.000,00
						TOTAL DA CONTRATAÇÃO (R$)	7.803.020,40

Item do Contrato	Descrição	Cálculo	Valor (R$)
Item 1	Proteção – 66 TB	118.500,00 ÷ 66 TB = 1.795,45 por TB	—
—	Proporção 50 TB para TJCE	1.795,45 x 50 TB*	**89.772,73**
Item 2	Franquia Adicional	1 TB = 1.000 GB × 1,30/GB	**1.300,00/TB**
Item 3	Proteção DNS	1.950,34÷ 5 Zonas**	**390,07 / Zona**

* foi considerado apenas 1 TB para encontrar o valor unitário aplicado ao quantitativo de 40 TB estimado para o TJCE

** foi considerado apenas 1 zona de DNS para encontrar o valor unitário aplicado ao quantitativo estimado para o TJCE

5. CUSTO TOTAL ESTIMADO

5.1. LOTE 1

Item	Nome	TJRO (F5 - 36 meses)	STJ (F5 - 60 meses)	TRF3/CJF (F5 - 60 meses)	TRF1 (A10 - 60 meses)	Média	Desvio padrão	Coeficiente de variação	Mediana	Mediana ou Média	UND
1	Solução ADC	R$ 980.000,00	R$ 955.454,57	R$ 1.467.800,00	R$ 1.021.638,00	R$ 1.106.223,14	R$ 210.092,79	19%	R$ 1.000.819,00	Média	Unidade
2	Suporte	R$ 12.000,00	R$ 5.119,55	R$ 13.000,00		R$ 10.039,85	R$ 3.503,05	35%	R$ 12.000,00	Mediana	MÊS
3	Treinamento	R$ 13.000,00	R$ 24.950,00	R$ 25.000,00	R$ 9.550,00	R$ 18.125,00	R$ 6.957,77	38%	R$ 18.975,00	Mediana	ALUNO
4	Instalação		R$ 65.750,00	R$ 88.000,00	R$ 40.000,00	R$ 64.583,33	R$ 19.613,27	30%	R$ 65.750,00	Mediana	Unidade

5.2. LOTE 2

Item	Nome	TRT-4 36 meses	TJRN 30 meses	SERPRO 36 meses	TRF3 60 meses	Média	Desvio padrão	Coeficiente de variação	Mediana	Média ou Mediana	UND	Qtde	Valo Unit

Item	Nome	TRT-4 36 meses	TJRN 30 meses	SERPRO 36 meses	TRF3 60 meses	Média	Desvio padrão	Coeficiente de variação	Mediana	Média ou Mediana	UND	Qtde	Valo Unit
1	Web Application Firewall (WAF) em modelo Software como Serviço (SaaS),com franquia mensal de 50 TB de tráfego inspecionado.	R$ 34.896,61	R$ 40.810,53	R$ 90.828,67	R$ 89.772,73	R$ 64.077,13	R$ 26.309,44	41%	R$ 65.291,63	Mediana	Mês	36	R$ 65.2
2	Franquia adicional de tráfego limpo a ser consumido e contratado sob demanda durante a vigência contratual	R$ 494,51	R$ 1.648,96	R$ 1.456,42	R$ 1.300,00	R$ 1.224,97	R$ 439,47	36%	R$ 1.378,21	Mediana	TB	900	R$ 1.37
3	Proteção DNS para 1 zona	R$ 490,05	R$ 1.402,36		R$ 390,07	R$ 896,22	R$ 506,15	56%	R$ 946,21	Mediana	Mês	36	R$ 946,2

5.3. CONSOLIDADO DO CUSTO TOTAL ESTIMADO

LOTE 1					
Id	**Bem/Serviço**	**UND**	**Qtd.**	**Vlr. Unitário**	**Vlr. Total**
1	Solução ADC	**UND**	**2**	**R$ 1.106.223,14**	**R$ 2.212.446,28**
2	Suporte	**MÊS**	**57**	**R$ 12.000,00**	**R$ 684.000,00**
3	Treinamento	**ALUNO**	**8**	**R$ 18.975,00**	**R$ 151.800,00**
4	Instalação	**UND**	**2**	**R$ 65.750,00**	**R$ 131.500,00**
Valor Total - LOTE 1					**R$ 3.179.746,28**

LOTE 2					
Id	**Bem/Serviço**	**UND**	**Qtd.**	**Vlr. Unitário**	**Vlr. Total**
1	Web Application Firewall (WAF) em modelo Software como Serviço (SaaS),com franquia mensal de 50 TB de tráfego inspecionado.	**Mês**	**36**	**R$ 65.291,63**	**R$ 2.350.498,68**
2	Franquia adicional de tráfego inspecionado a ser consumido e contratado sob demanda durante a vigência contratual	**TB**	**900**	**R$ 1.378,21**	**R$ 1.240.389,00**
3	Proteção DNS para 1 zona	**Mês**	**36**	**R$ 946,21**	**R$ 34.063,56**
Valor Total - LOTE 2					**R$ 3.624.951,24**
CUSTO TOTAL ESTIMADO					**R$ 6.804.697,52**

6. CONCLUSÃO DA PESQUISA DE PREÇOS

6.1. Conclui-se que o valor estimado da contratação foi definido com base em pesquisa de preços realizada a partir de fontes idôneas e compatíveis com o objeto, refletindo os valores praticados no mercado para soluções de características equivalente, não tendo sido identificados indícios de sobrepreço ou inexequibilidade nos valores analisados.

6.2. Assim, entende-se que o valor estimado é adequado para subsidiar a presente contratação, em observância aos princípios da economicidade, da razoabilidade e do planejamento, nos termos do art. 5º da Lei nº 14.133/2021.

7. APROVAÇÃO e ASSINATURA

Fortaleza, na data da assinatura eletrônica

Max Eduardo Vizcarra Melgar – 48994 Integrante Técnico	Matheus Freire e Silva do Nascimento - 50707 Integrante Requisitante	Francisco José Pessoa Furtado – 8284 Integrante Administrativo

Documento assinado eletronicamente por **MAX EDUARDO VIZCARRA MELGAR**, **Gestor de Unidade**, em 22/06/2026, às 14:54, 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 22/06/2026, às 15:40, 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**, **Servidor**, em 22/06/2026, às 15:59, 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 **0765122** e o código CRC **F6DD06EF**.

Referência: Processo nº 8515550-95.2025.8.06.0000 SEI nº 0765122