CONTRATAÇÃO DE PRESTAÇÃO DE SERVIÇOS DE FIREWALL DE APLICAÇÃO WEB (WEB APPLICATION FIREWALL 3 WAF), NA MO DALIDADE SOFTWARE COMO SERVIÇO (SAAS) CONTÍNUO, PELO PERÍODO DE 36 (TRINTA E SEIS) MESES, INCLUINDO SUBSCRIÇÃO, IMPLANTAÇÃO, CONFIGURAÇÃO E SUPORTE TÉCNICO ESPECIALI ZADO (LOTE 2).

Nº 55/2026

ORIGEM:
Secretaria da Tecnologia da Informação

PROCESSO ADMINISTRATIVO:
8515550-95.2025.8.06.0000

LOTE 02 (SEI nº 8525044-72.2026.8.06.0000)

CÓDIGO DA CONTRATAÇÃO (PAC):
RDP-SETIN-2026-26

CONTRATANTE: O TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, situado no Centro Administrativo Governador Virgílio Távora, com sede na Avenida General Afonso Albuquerque Lima, S/N, Bairro Cambeba, Fortaleza – CE, inscrito no CNPJ sob o número 09.444.530/0001-01, doravante denominado simplesmente de **TJCE** ou **CONTRATANTE**, neste ato representado por seu Presidente, Desembargador Heráclito Vieira de Sousa Neto e por sua Secretária de Tecnologia da Informação do TJCE, Denise Maria Norões Olsen, e **CONTRATADA: ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA.**, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 10.864.910/0001-76, e sediada na Av. Marcos Penteado de Ulhoa Rodrigues, nº 939 Edifício Jacarandá Sala 882, São Paulo/SP, neste ato representada pelo seu Representante Legal, Sr. Leandro Manoel Aparício, inscrito no CPF sob o nº 214.XXX.XXX-70, daqui por diante simplesmente denominada **CONTRATADA**.

Pelo presente instrumento particular, os acima qualificados e abaixo assinados resolvem de comum acordo, celebrar o presente contrato, que está vinculado ao instrumento convocatório da respectiva licitação, bem como à proposta da CONTRATADA e se regerá pela Lei Federal nº 14.133/21 com suas alterações, pela Resolução n. 468 de 15 de julho de 2022 e atualizações posteriores e pelas seguintes cláusulas e condições, que mutuamente se obrigam a cumprir:

CLÁUSULA PRIMEIRA – DO OBJETO

1. O objeto deste instrumento consiste na Contratação de prestação de serviços de Firewall de Aplicação Web (Web Application Firewall 3 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), com vistas a garantir a disponibilidade, a segurança e o desempenho dos serviços digitais do Tribunal de Justiça do Estado do Ceará (TJCE), conforme especificações, quantitativos e exigências estabelecidas no Edital do Pregão Eletrônico n. 32/2026 e seus anexos.

1.1 Vinculam esta contratação, independentemente de transcrição:
1.1.1 Termo de Referência;
1.1.2 Edital do Pregão Eletrônico n. 32/2026 e seus anexos;
1.1.3 Proposta do contratado;
1.1.4 Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – FORMA DE EXECUÇÃO E REGIME

2. O objeto do presente contrato será executado no regime de empreitada por preço global, conforme especificações contidas no Edital do Pregão Eletrônico n. 32/2026 e seus anexos, bem como nos Anexos deste Contrato.

CLÁUSULA TERCEIRA – DO VALOR

3. O presente contrato possui valor global de **R$ 2.774.998,80 (dois milhões, setecentos e setenta e quatro mil, novecentos e noventa e oito reais e oitenta centavos)**, para todo o período contratado, respeitando os valores elencados no **ANEXO 2 do Edital**, sendo devidos somente os valores respectivos aos objetos efetivamente recebidos, na forma e proporção do recebimento, medição e avaliação da qualidade, conforme **ANEXO 1 do Edital (Termo de Referência).**

3.1 INCLUSÕES NO PREÇO - Todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto e, ainda, todos e quaisquer tributos, taxas, contribuições e/ou encargos trabalhistas e previdenciários, horas extras, impostos incidentes, direta ou indiretamente, lucro, embalagens, e demais custos relacionados ao objeto deste contrato serão de exclusiva responsabilidade da **CONTRATADA** e estão incluídos nos preços.

3.1.1 Serão de exclusiva responsabilidade da **CONTRATADA** quaisquer outros custos que incidam, direta ou indiretamente, sobre o presente contrato, necessários para a realização do seu objeto, tais como: supervisão, direção, administração, mão-de-obra, adicional de periculosidade, horas extras, fornecimento de materiais previamente definidos, equipamentos, ferramentas, combustíveis, EPIs, transporte de pessoal, despesas com viagens e estadias, licenças, insumos, além de outros custos resultantes de outras obrigações legais, inclusive lucro da **CONTRATADA**, não cabendo quaisquer reivindicações posteriores, a título de revisão de preço ou reembolso, seja a que título for.

CLÁUSULA QUARTA – DA ATUALIZAÇÃO DE PREÇOS

4. Exceto na hipótese de condições supervenientes ou estabelecidas por órgãos governamentais competentes, o(s) preço(s) deste contrato não sofrerá(ão) reajuste no primeiro ano de vigência de cada parcela do preço segundo sua data-base. Decorridos mais de 12 (doze) meses da respectiva data base, os preços deste contrato poderão ser atualizados mediante:

4.1 REAJUSTE Independente de pedido formal da Contratada, será admitido o REAJUSTE do valor do contrato, com base no Índice de Custos de Tecnologia da Informação – ICTI, divulgado pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA, observado o interregno mínimo de 1 (um) ano de acordo com a variação do ICTI a partir da data do orçamento estimado desta contratação, condições e critérios estabelecidos no **item 14 do Anexo 1 do Edital – Termo de Referência**.

4.1.1 O processo para análise de reajuste deverá ser aberto em tempo hábil pelo Fiscal deste Contrato e firmado pelo Gestor.

4.2 REVISÃO DE PREÇO - Se, durante o prazo de vigência do contrato, ocorrer a criação ou extinção de tributos, independentemente do período de tempo decorrido, alteração ou redução de alíquota ou instituição de estímulos fiscais de qualquer natureza e isenção ou redução de tributos federais, estaduais e municipais que comprovadamente venha a majorar ou diminuir os ônus do presente contrato, os preços poderão ser revistos a fim de adequá-los às modificações havidas, compensando-se, na primeira oportunidade seguinte de pagamento, quaisquer diferenças decorrentes dessas alterações havidas entre a data do fato gerador e a decisão de atualização financeira por revisão.

4.2.1 Caberá revisão de preços para restabelecer a relação que as partes pactuaram inicialmente entre os encargos da **CONTRATADA** e a retribuição do **TJCE** para a justa remuneração da obra, serviço ou fornecimento, objetivando a manutenção do equilíbrio econômico-financeiro inicial do contrato, na hipótese de sobrevirem fatos imprevisíveis, ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado;

4.2.1.1 Também será admitida a revisão de preço(s) prevista neste subitem em caso de força maior, caso fortuito ou fato do príncipe, que configurem álea econômica extraordinária e extracontratual.

4.3 **O prazo para resposta ao pedido de reequilíbrio será o total de 31 (trinta e um) dias úteis**, contados da data do fornecimento pela contratada da demonstração analítica da variação dos custos.

4.4 PRECLUSÃO TEMPORAL - Quando de interesse da **CONTRATADA**, para que seja promovida a revisão, deverá esta apresentar pedido formal escrito e fundamentado acompanhado das comprovações de impacto efetivo nos seus custos no prazo de **até 90 (noventa) dias** da

ocorrência do fato gerador, e não terá efeito retroativo em relação aos pagamentos já cobrados com nota fiscal emitida, sendo que pedidos promovidos em momento posterior ao fixado nesta cláusula retroagirão seus efeitos até o máximo de 90 (noventa) dias anteriores ao pedido.

4.5 PRECLUSÃO LÓGICA - Caso haja formalização de aditivo contratual de qualquer natureza, sem expressa ressalva à atualização anterior ou pendente, esta deixará de ser devida e o(s) preço(s) do contrato permanecerá(ão) o(s) vigente(s) e receberá(ão) nova data-base igual à do aditivo porventura firmado.

4.6 ATUALIZAÇÃO DE ITENS ADICIONADOS AO OBJETO – Caso sejam adicionados itens novos ao contrato, não contemplados originalmente no **ANEXO II do Edital (Orçamento Detalhado)**, estes terão como data-base e princípio de contagem de prazo para reajustamento a data do respectivo aditivo de inclusão.

CLÁUSULA QUINTA – DA FORMA DE PAGAMENTO

5. Os pagamentos decorrentes do presente contrato serão promovidos nas exatas proporções e preços do que for efetivamente demandado, recebido e aceito, conforme qualidade avaliada, e serão efetuados através de transferência ou depósito na conta bancária de titularidade da **CONTRATADA,** seguindo, ainda, o previsto no **item 8.4 do Anexo 1 do Edital (Termo de Referência)**.

5.1 GERAÇÃO DA NOTA FISCAL - As cobranças só poderão ser promovidas após as respectivas notas fiscais terem sido aprovadas pelo **TJCE**, na proporção dos serviços executados e recebidos e desde que acompanhada dos documentos exigidos por conta deste contrato.

5.1.1 A Nota Fiscal correspondente aos serviços prestados **deverá observar o CNPJ indicado na Nota de Empenho**.

5.2 DATA LIMITE PARA EMISSÃO DA NOTA FISCAL - As Notas Fiscais devem ser emitidas e encaminhadas após o recebimento definitivo do objeto, mediante comunicação do gestor do contrato.

5.3 CONTEÚDO DA NOTA FISCAL - A emissão dos documentos fiscais e de transporte deve respeitar as indicações porventura fornecidas pelo **TJCE**, devendo constar, além das informações essenciais legais e usuais para o tipo de documento, o número do contrato e o telefone do **TJCE**, quando exigido em campo próprio de emissão da nota fiscal eletrônica, e ainda, quando previsto no **ANEXO 1 (Termo de Referência**), a indicação do nível de serviço ou medição de resultado que determine o critério de apuração do valor de pagamento devido.

5.3.1 CONTA PARA RECEBIMENTO - Os dados bancários da **CONTRATADA** devem ser informados na nota fiscal e, na impossibilidade, através de outro meio formal escrito, apresentado ao **TJCE**, sendo condição suspensiva para realização dos pagamentos.

5.3.2 ENVIO ELETRÔNICO DA NOTA FISCAL - Como condição suspensiva para o pagamento, deverá a **CONTRATADA,** junto com as notas fiscais apresentadas, enviar e-mail para o gestor ou fiscal de contratos indicado pelo **TJCE** contendo a Nota Fiscal / DANFE em arquivo PDF e o respectivo arquivo XML gerado no sistema emissor da Nota Fiscal.

5.3.2.1 DOCUMENTOS ADICIONAIS E AUXILIARES DA NOTA FISCAL - Havendo exigência legal adicional com geração de documento decorrente do objeto executado deste contrato, como documentos auxiliares, seja de exigência geral e nacional, ou específica e regional, deverá a **CONTRATADA** adicionar aos envios previstos neste item, sempre no formato original de geração, preferencialmente XML, e em PDF.

5.3.2.2 EXCEÇÃO DE EXIGÊNCIA DE ENVIO ELETRÔNICO - Excepcionalmente, em caso de integração de sistemas eletrônicos, e a critério do **TJCE**, pode ser dispensada a **CONTRATADA** de encaminhar um ou mais documentos abrangidos neste item, dispensa esta que só valerá se comunicada formalmente por escrito pelo **TJCE**.

5.4 CONDIÇÃO GERAL SUSPENSIVA DE PAGAMENTO - A cada cobrança e como condição de pagamento, a **CONTRATADA** deverá obrigatoriamente comprovar sua regularidade fiscal, através da entrega dos documentos abaixo:

5.4.1 Prova de regularidade para com a Fazenda Federal e quanto à Dívida Ativa da União, bem como àquela relativa à Seguridade Social, do seu domicílio ou sede, através da Certidão Conjunta, emitida pela Secretaria da Receita Federal, incluindo as contribuições sociais;

5.4.2 Prova de regularidade para com a Fazenda Estadual do seu domicílio ou sede;

5.4.3 Prova de regularidade para com a Fazenda Municipal do seu domicílio ou sede;

5.4.4 Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS), mediante a apresentação do Certificado de Regularidade do FGTS – CRF;

5.4.5 Certidão Negativa de Débitos Trabalhistas (CNDT).

5.5 NATUREZA JURÍDICA DAS CONDIÇÕES - As condições acima listadas tem natureza suspensiva e não se confundem com retenção de pagamentos, de modo que enquanto não atendidas as condições acordadas acima para que a **CONTRATADA** torne-se credora de parcela do contrato, não haverá qualquer valor devido, e, uma vez atendidas todas as condições estabelecidas acima, a **CONTRATADA** tornar-se-á credora e deverá receber sua remuneração contando-se o prazo de vencimento a partir da data de regularização documental e cumprimento da condição.

5.6 PRAZO DE PAGAMENTO - As notas fiscais aprovadas pelo **TJCE** serão liquidadas em até **30 (trinta)** dias corridos, contados da data do ateste da nota fiscal pelo **TJCE**, que depende do recebimento definitivo do objeto e a confirmação de recebimento de todos os documentos exigidos por conta deste contrato.

5.6.1 ATRASO DE PAGAMENTO - Ante eventual atraso de pagamento, será devida atualização monetária entre a data do vencimento e a do efetivo pagamento, com base na mesma regra de reajuste acima.

5.6.2 INTERRUPÇÃO DE PRAZO DE PAGAMENTO - O prazo de pagamento da nota fiscal será interrompido na hipótese de serem constatados erros, falhas ou irregularidades, ou quando estas não estiverem acompanhadas de documentos exigidos nesta cláusula, iniciando a fluir, na sua integralidade, a partir da apresentação de nova nota fiscal correta e da apresentação dos documentos exigidos e após aprovação/ateste pelo **TJCE**, sem prejuízo da continuidade do contrato.

5.6.2.1 IRREGULARIDADE – 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 apresente justificativa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do TJCE. Persistindo a irregularidade, o TJCE poderá adotar as medidas necessárias à extinção do Contrato, bem como a possibilidade de contratação de remanescente.

5.6.3 DESCONTOS AUTORIZADOS - O **TJCE** poderá deduzir dos valores a serem pagos à **CONTRATADA** quaisquer quantias que lhe forem devidas por esta, promovendo a devida compensação, como, por exemplo, multas por inadimplemento contratual, prejuízos causados pela **CONTRATADA** ou dispêndio por força de condenação subsidiária ou solidária em processos judiciais e/ou extrajudiciais que tenham por base ato ou pessoa do grupo de empregados da **CONTRATADA** e quaisquer outros débitos, além das disposições previstas no **item 8 do Anexo 1 do Edital (Termo de Referência)**.

5.6.4 DESCONTOS FISCAIS - O **TJCE**, na qualidade de fonte retentora, descontará e recolherá, nos prazos da Lei, dos pagamentos que efetuar à **CONTRATADA**, os tributos a que esteja obrigada pela legislação vigente.

5.6.5 COMPROVAÇÃO DE ENQUADRAMENTO NO SIMPLES – Caso a **CONTRATADA** seja optante do Simples Nacional, deverá apresentar juntamente com a nota fiscal, declaração ou extrato da consulta atualizada de condição fiscal, respeitando enquadramento correto e normas aplicáveis da Receita Federal, afirmando que está enquadrada no Simples com indicação exata do Anexo que se enquadre.

5.6.6 COMPROVAÇÃO DE IMUNIDADE TRIBUTÁRIA – Caso a **CONTRATADA** tenha enquadramento que lhe confira imunidade tributária, deverá apresentar juntamente com a nota fiscal – ou descrito no corpo dela – declaração desta condição especial com indicação de fundamentos.

5.6.7 PROIBIÇÃO DE CESSÃO – A **CONTRATADA** não poderá fazer cessão dos créditos decorrentes deste contrato, salvo com concordância prévia e formal do TJCE.

5.7 DOTAÇÃO ORÇAMENTÁRIA – Os recursos financeiros correrão por conta do Fundo Especial de reaparelhamento e Modernização do Poder Judiciário do Estado de Ceará – **FERMOJU**, tendo como fonte os Recursos Diretamente Arrecadados, nas seguintes dotações orçamentárias:

04200021.02.126.192.11470.15.449040.1.759.1200070.1.2.01
04200021.02.126.192.11470.15.449040.2.759.1200070.1.2.01
04200021.02.126.192.11470.15.449052.1.759.1200070.1.2.01
04200021.02.126.192.11470.15.449052.2.759.1200070.1.2.01
04200021.02.126.192.20511.15.339040.1.759.1200070.1.2.01
04200021.02.126.192.20511.15.339040.2.759.1200070.1.2.01

CLÁUSULA SEXTA – DAS OBRIGAÇÕES DA CONTRATADA

6. Além das demais obrigações estipuladas neste contrato, no **item 5.2 do Anexo 1 do Edital (Termo de Referência)** e na legislação aplicável, está obrigada a **CONTRATADA** a:

6.1 RESPONSABILIDADE EXECUTIVA - Planejar, conduzir e executar os serviços com integral atendimento das especificações e prazos estabelecidos neste contrato e no **ANEXO 1 do Edital (Termo de Referência),** aplicando elevado padrão de qualidade e confiabilidade, bem como não realizar nenhuma modificação nas especificações dos equipamentos e serviços sem a prévia autorização do **TJCE**;

6.2 GARANTIA, MANUTENÇÃO E ASSISTÊNCIA TÉCNICA – Seguir todas as condições, prazos e orientações de Garantia, Manutenção e Assistência Técnica estabelecidas no **item 4.14 do Anexo 1 do Edital (Termo de Referência).**

6.3 CONDIÇÕES DE EXECUÇÃO E RECEBIMENTO: Seguir todas as condições, prazos e orientações definidas para a execução e recebimento dos serviços, dispostas nos **itens 6, 7, 8, 9, 10 e 11 do Anexo 1 do Edital (Termo de Referência).**

6.4 PARÂMETROS EXTRACONTRATUAIS – Respeitar as Leis Federais, Estaduais e Municipais relacionadas à realização dos serviços, assim como normas técnicas aplicadas ao objeto da contratação, isentando o **TJCE** de qualquer responsabilidade pela inobservância de disposições aplicáveis;

6.5 NOMEAÇÃO DE PREPOSTO – Constituir formalmente preposto(s) para representá-la na execução do contrato e nas reuniões de definição operacional, através de instrumento escrito conforme modelo do **ANEXO IV do Termo de Contrato (Termo de Nomeação de Preposto)**, salvo se a **CONTRATADA** alocar diretamente nas atividades representante legal instituído pelos documentos de constituição da pessoa jurídica;

6.6 DIREÇÃO DOS TRABALHOS – Promover supervisão e direção administrativa e técnica na execução do objeto do contrato;

6.7 REGULARIDADE LEGAL – Cumprir todas as leis aplicáveis e efetuar o pagamento de todos os tributos devidos relacionados à sua atividade (federais, estaduais e municipais) e encargos sociais e/ou previdenciários, assim como remuneração e benefícios de seus empregados ou prepostos;

6.8 INDENIZAÇÕES - Indenizar o **TJCE** e/ou terceiros por quaisquer danos ou prejuízos causados por seus representantes legais, empregados ou prepostos, por ação ou omissão, bem como por defeito ou falta de qualidade do serviço executado e mesmo por decorrência de retardo, assim como por quaisquer despesas, judiciais ou extrajudiciais, decorrentes da execução das atividades deste contrato, bem como requerer imediata exclusão do **TJCE** de qualquer lide que tenha sido integrada por força de ato ou empregado da **CONTRATADA** ou subcontratada, isentando o **TJCE** de quaisquer ônus porventura havido e indenizando os porventura já ocorridos, tais como custas judiciais, honorários advocatícios e despesas, judiciais e extrajudiciais, devidamente comprovadas, relativas às defesas ou comparecimento em solenidades judiciais;

6.9 HABILITAÇÃO E QUALIFICAÇÃO – Manter durante toda a vigência contratual, as condições de habilitação e qualificação exigidas no procedimento licitatório ou na contratação direta;

6.10 INCONFORMIDADES NA ESPECIFICAÇÃO – Comunicar formalmente ao **TJCE** sobre quaisquer erros, omissões, incorreções ou discrepâncias que, porventura, sejam encontrados em projetos ou especificações de pedidos ou de descrição do objeto;

6.11 SIGILO – Manter sigilo sobre todas as informações obtidas por decorrência do presente contrato, sendo proibido reproduzir ou encaminhar a terceiros, salvo se previamente autorizado pelo TJCE;

6.11.1 O representante da **CONTRATADA** tomará conhecimento do **TERMO DE COMPROMISSO DE SIGILO E NORMAS DE SEGURANÇA** e assinará o documento, **ANEXO I deste Contrato**, juntamente com este contrato.

6.12 FISCALIZAÇÃO – Permitir acesso do **TJCE** em qualquer local onde seja executado serviço para fins de fiscalização e auditoria administrativa e técnica;

6.13 ADEQUAÇÃO TRABALHISTA – Não utilizar mão de obra em desacordo com as normas legais que tratam do combate à discriminação de raça, gênero, direção/orientação sexual e religião, ao trabalho infantil e ao trabalho escravo, assim como observar e fazer cumprir rigorosamente todas as leis trabalhistas, previdenciárias, tributárias e outras aplicáveis por conta do emprego de profissionais na execução das atividades, além das normas coletivas da(s) categoria(s) envolvidas;

6.14 AJUSTE DE TRABALHOS – Atender prontamente as recomendações do **TJCE** no sentido de alterar os métodos empregados na execução dos serviços, caso os métodos originalmente estabelecidos se mostrem inadequados ou ineficientes para o cumprimento dos prazos e resultado satisfatório na execução dos serviços, sem quaisquer custos adicionais, podendo negar-se a fazê-lo apenas quando a determinação do **TJCE** significar descumprimento à Lei ou norma técnica de execução ou a alteração for de significativo impacto em custos;

6.15 EQUIPE DE TRABALHO – Quanto à equipe responsável pela execução dos serviços objeto do presente contrato, cabe obrigatoriamente à **CONTRATADA:**

6.16 Recrutar em seu nome e sob sua inteira responsabilidade os profissionais necessários para execução do objeto do contrato;

6.16.1 Manter, durante a vigência do contrato, equipe composta por profissionais devidamente capacitados e treinados nas atividades que lhes forem incumbidas, devidamente identificados, possibilitando o adequado cumprimento do objeto deste contrato;

6.16.2 Respeitar as regras de acesso às instalações do TJCE e orientar os profissionais para que não transitem ou permaneçam em áreas diferentes daquelas indicadas e permitidas pelo **TJCE**, para acesso e execução dos serviços;

6.16.3 Manter o registro dos seus empregados permanentemente atualizado em formato admitido pelo Ministério do Trabalho, apresentando prontamente ao TJCE, sempre que solicitado pela mesma, bem como e as anotações da Carteira Profissional de cada empregado;

6.16.4 Assumir, direta e exclusivamente, responsabilidade pelos danos causados em acidentes de trabalho, ou acidentes envolvendo terceiros, que eventualmente venham a ocorrer por conta da execução do objeto deste contrato;

6.16.5 Responsabilizar-se pelo transporte dos profissionais alocados no trabalho, inclusive em casos de paralisação de transportes coletivos, bem como nas situações em que se faça necessária a execução do contrato em regime extraordinário;

6.16.6 Disponibilizar acesso a todos empregados, documentação relativa ao cumprimento das obrigações de natureza trabalhista, previdenciária, fiscal, técnica, entre outras, referentes aos profissionais da equipe alocada neste contrato, insumos utilizados e trabalhos realizados, bem como a sistemas públicos ou privados que guardem informações relevantes sobre a regularidade trabalhista da CONTRATADA;

6.16.7 Observar e fazer cumprir a política de gestão integrada do **TJCE**

6.17 CORREÇÃO DE DEFEITOS OU FALHAS – Corrigir quaisquer defeitos ou falhas nos serviços executados e substituir materiais porventura fornecidos que apresentarem qualquer tipo de falha ou impropriedade para a aplicação pretendida, inclusive durante a garantia técnica prevista nos **itens 4.14, 8 e 12 do Anexo 1 do Edital (Termo de Referência);**

6.17.1 EXECUÇÃO DIRETA INDENIZÁVEL – Em caso de descumprimento de obrigação prevista neste subitem, poderá o **TJCE** executar, direta ou indiretamente, o objeto do contrato ou a correção necessária, cobrando as despesas correspondentes, devidamente corrigidas, permitida a retenção de créditos da **CONTRATADA**.

6.18 TRANSIÇÃO DO SERVIÇOS PRESTADOS – Repassar, quando do período de transição inicial e/ou final do contrato, ou quando solicitado pelo **TJCE**, aos profissionais indicados pelo **TJCE**, os documentos, procedimentos e demais informações necessárias para continuidade dos serviços prestados na vigência do contrato.

6.19 SUSTENTABILIDADE – Atuar de forma que suas ações, direta ou indiretamente, relacionadas a este contrato, atendam às normas ambientais pertinentes e de segurança, adotando formas de intervenção que evitem o impacto ambiental ou acidentes de quaisquer naturezas, em cumprimento às orientações e diretrizes do **TJCE**, legislação vigente e requisitos de sustentabilidade dispostos no **item 4.19.1 do Anexo 1 do Edital (Termo de Referência);**

6.20 **UTILIZAÇÃO E DEVOLUÇÃO DE MATERIAIS E EQUIPAMENTOS** – Guardar e manusear cuidadosamente os materiais e equipamentos que porventura sejam disponibilizados pelo **TJCE** para a execução dos serviços, obrigando-se a repor, por sua conta exclusiva e sem prejuízo dos prazos estipulados, aqueles que, sob sua guarda, forem danificados ou extraviados, obrigando-se a devolver o acervo remanescente ao final de cada utilização ou do prazo de vigência do contrato, conforme seja requerido pelo **TJCE**;

6.21 **CREDENCIAIS DE ACESSO AO SISTEMA** – Zelar pela utilização restrita das credenciais de acesso – login e senha – aos sistemas do **TJCE** de modo que só sejam utilizadas por representante da **CONTRATADA** devidamente autorizado, comprometendo-se em trocar a senha de acesso, gerenciar e atualizar seus usuários, e avisar imediatamente qualquer suspeita de indevida utilização de acesso.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DO TJCE

7. Além das demais obrigações estipuladas neste Termo de Contrato, no **item 5.1** do **Anexo 1 do Edital (Termo de Referência)** e na legislação aplicável, caberá ao **TJCE**:

7.1 GARANTIA DE ACESSO - Permitir o acesso da **CONTRATADA** aos materiais e/ou locais necessários à execução e entrega do(s) objeto(s) contratado(s), desde que atendidos os pré-requisitos, normativos ou exigidos neste contrato e seus anexos, para liberação de acesso;

7.2 Fornecer local para a guarda de materiais, equipamentos e utensílios da **CONTRATADA**;

7.3 Disponibilizar à **CONTRATADA** normas e regulamentos internos aplicáveis aos locais de entrega.

7.4 Designar responsáveis para o acompanhamento e fiscalização da execução do objeto contratual, informando à **CONTRATADA** sobre quaisquer atos que possam interferir direta ou indiretamente na prestação dos serviços.

7.5 Solicitar a prestação dos serviços por meio de contrato.

7.6 Enviar por e-mail a lista de priorização dos serviços de instalação à Contratada, contendo as informações necessárias à execução do objeto.

7.7 Receber os serviços que atenderem aos requisitos deste termo de referência e do edital.

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

7.9 Proporcionar todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do contrato, consoante estabelece a Lei Federal 14.133/21 e suas alterações.

7.10 Acompanhar, fiscalizar, conferir e verificar a execução do contrato, por meio de sua unidade competente, podendo, em decorrência, solicitar providências da Contratada, que atenderá ou justificará de imediato.

7.11 Notificar a Contratada acerca de eventual irregularidade decorrente da execução do objeto cujo preço encontra-se registrado, fixando prazo para sua correção.

7.12 Rejeitar, no todo ou em parte, o serviço prestado em desacordo com as obrigações assumidas pela Contratada, indicando as razões da recusa.

7.13 Proceder à verificação de relatório dos chamados de suporte técnico para aplicação de eventuais glosas no pagamento mensal dos serviços.

7.14 Atestar a nota fiscal/fatura apresentada pela Contratada.

7.15 Determinar a retificação de dados pela Contratada sempre que forem detectadas inconsistências nos seus documentos fiscais.

7.16 Efetuar os pagamentos devidos à Contratada nas condições estabelecidas neste termo.

7.17 Aplicar as penalidades previstas em lei e neste instrumento.

CLÁUSULA OITAVA – DOS CASOS OMISSOS

8. Os casos omissos serão decididos pelo **TJCE**, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA NONA - DAS ALTERAÇÕES DESTE CONTRATO

9. O presente contrato poderá ser alterado por acordo entre as partes ou unilateralmente pelo TJCE na forma e nos limites dos arts. 124 a 136 da Lei nº 14.133/21.

9.1 CLÁUSULA DE QUITAÇÃO – Em qualquer caso de aditivo, será adicionada a seguinte cláusula de quitação ao instrumento de aditamento contratual:

9.1.1 "A **CONTRATADA** dá ao **TJCE**, neste ato, plena, rasa e geral quitação de todas as obrigações correspondentes ao período compreendido entre o início da vigência contratual até a presente data, relativos ao contrato acima mencionado, para nada reclamar, sob qualquer título ou pretexto, em juízo ou fora dele".

9.1.2 Caso exista alguma obrigação pendente de pagamento ou análise financeira em possível proveito à **CONTRATADA**, poderá ser objeto de ressalva na cláusula de quitação, acrescendo-se, ao final do texto acima a continuação:

", ressalvando-se o(s) pagamento(s) pendente(s) relacionado a: _____"

9.2 HIPÓTESES DE ALTERAÇÃO POR ACORDO, especialmente nos seguintes casos:

9.2.1 quando conveniente a substituição da garantia de execução;

9.2.2 quando necessária a modificação do regime de execução do serviço, bem como do modo de fornecimento, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;

9.2.3 quando necessária a modificação da forma de pagamento por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado e vedada a antecipação do pagamento em relação ao cronograma financeiro fixado sem a correspondente contraprestação de fornecimento de bens ou execução do serviço;

9.2.4 para restabelecer o equilíbrio econômico-financeiro inicial do contrato em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato.

9.3 AJUSTES PRÉ-ACORDADOS - A **CONTRATADA** concorda em manter estrutura capaz para adição de objeto e admite desde já acréscimos quantitativos nas mesmas condições deste contrato até o limite acima estabelecido.

CLÁUSULA DÉCIMA - DA VIGÊNCIA

10. O presente contrato terá vigência de 36 (trinta e seis) meses, contados a partir da data de assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

10.1 A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com a **CONTRATADA**.

10.2 A **CONTRATADA** não tem direito subjetivo à prorrogação contratual.

10.3 A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

10.4 O contrato não poderá ser prorrogado quando a CONTRATADA tiver sido penalizada nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

10.5 A garantia integral da solução contratada durante toda a vigência do contrato, contemplando equipamentos, peças, insumos e serviços, sem qualquer ônus adicional para o TJCE, observadas as demais condições estabelecidas **no item 12** do **Anexo 1 do Edital (Termo de Referência)**.

10.6 **PRAZO DE EXECUÇÃO DO CONTRATO –** O(s) prazo(s) de execução se darão conforme previsto no **ANEXO 1 do Edital (Termo de Referência).**

10.6.1 Não é obrigatória a concessão de extensão do prazo de execução caso o **TJCE** recuse o objeto(s) em desacordo com o projeto e/ou especificações, cabendo a esta decidir se concede prazo adicional para regularização, aplica sanções e/ou rescinde o presente contrato.

CLÁUSULA DÉCIMA PRIMEIRA – DAS PENALIDADES

11. Quanto às penalidades, deve-se observar o disposto nesta cláusula, no **item 8.3 do Anexo 1 do Edital (Termo de Referência)** e na legislação aplicável.

11.1 Ante eventual inadimplemento na execução deste contrato, a **CONTRATADA** estará sujeita às seguintes sanções administrativas, conforme previsto no artigo 156 da Lei 14.133/21:

11.1.1 Advertência;

11.1.2 Multa;

11.1.2.1 A multa moratória será aplicada nos casos de atraso injustificado no cumprimento das obrigações contratuais cujos prazos estejam expressamente previstos neste Termo de Referência.

11.1.2.2 A multa moratória corresponderá a 0,5% (cinco décimos por cento) por dia de atraso, incidente sobre o valor da parcela inadimplida, até o trigésimo dia de atraso, passando a 0,7% (sete décimos por cento) por dia para cada dia subsequente, observados os limites estabelecidos no Manual para Aplicação de Penalidades do Tribunal de Justiça do Estado do Ceará.

11.1.2.3 A contagem do atraso injustificado iniciar-se-á no primeiro dia de expediente subsequente ao término do prazo contratualmente previsto para cumprimento da obrigação, sendo computada, a partir do termo inicial, em dias corridos, inclusive aqueles sem expediente.

11.1.2.4 O atraso injustificado superior a 20 (vinte) dias no cumprimento de obrigação principal poderá caracterizar inexecução parcial ou total do contrato, conforme a extensão do inadimplemento e os prejuízos causados à Administração, hipótese em que a multa moratória poderá ser convolada em multa compensatória, sem prejuízo da adoção das demais medidas administrativas cabíveis, inclusive rescisão contratual, observado o contraditório e a ampla defesa.

11.1.2.5 A multa compensatória poderá ser aplicada nos casos de inexecução parcial ou total do contrato, paralisação injustificada da execução dos serviços, reincidência de falhas operacionais relevantes, descumprimento reiterado dos níveis mínimos de serviço estabelecidos no Instrumento de Medição de Resultado (IMR) ou descumprimento grave das obrigações contratuais, inclusive após a caracterização da hipótese prevista no subitem 8.3.5 do **Anexo 1 do Edital (Termo de Referência)**.

11.1.2.6 O descumprimento reiterado dos níveis mínimos de serviço estabelecidos no Instrumento de Medição de Resultado – IMR poderá ensejar aplicação das penalidades previstas neste Termo de Referência, observada a gravidade da ocorrência, reincidência, impactos operacionais causados à Administração e contraditório da contratada, sem prejuízo da aplicação das sanções previstas nos itens 8.3 do **Anexo 1 do Edital (Termo de Referência)**.

11.1.2.7 A estipulação de multas por atraso não significa que o **TJCE** vai aceitar serviços em retardo, ficando a seu critério aceitar em atraso, aplicando a multa de mora, ou extinguir o contrato por descumprimento, a qualquer momento de eventual atraso.

11.1.2.8 As multas que por porventura a **CONTRATADA** der causa poderão ser descontadas de pagamentos eventualmente devidos pelo **TJCE**, ou ainda por outro meio que satisfaça a liquidação do débito, inclusive descontado da garantia, podendo ser cobradas judicialmente caso não haja suficiência e satisfação nos meios originalmente indicados;

11.1.2.9 Adicionalmente a estas multas acima pré-fixadas, recairá ainda sobre eventual inexecução total ou parcial as multas ou graduação porventura previstas para casos específicos no Edital, Termo de Referência ou em anexo específico deste contrato.

.

11.1.3 Impedimento de licitar e contratar;

11.1.4 Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

11.2 Na aplicação das sanções serão considerados:

11.2.1 a natureza e a gravidade da infração cometida;

11.2.2 as peculiaridades do caso concreto;

11.2.3 as circunstâncias agravantes ou atenuantes;

11.2.4 os danos que dela provierem para o **TJCE**;

11.2.5 a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

11.3 Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente.

11.4 A personalidade jurídica da **CONTRATADA** poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

11.5 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação, na forma do art. 163 da Lei nº 14.133/21.

11.6 NÃO LIMITAÇÃO E OBRIGAÇÃO DE INDENIZAR - As penalidades estabelecidas nesta cláusula não excluem quaisquer outras previstas em Lei, nem a responsabilidade da **CONTRATADA** por perdas e danos que causar ao **TJCE** em consequência do inadimplemento, que poderão ser cobradas a qualquer tempo.

CLÁUSULA DÉCIMA SEGUNDA – DA EXTINÇÃO

12. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

12.1. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o **TJCE**, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

12.2. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação da **CONTRATADA** pelo **TJCE** nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

12.3. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

12.4. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

CLÁUSULA DÉCIMA TERCEIRA – DA SUBCONTRATAÇÃO

13. A **CONTRATADA** não poderá subcontratar, ceder ou transferir o objeto do contrato.

CLÁUSULA DÉCIMA QUARTA – DA GARANTIA FINANCEIRA

14. A **CONTRATADA** deverá submeter à Coordenadoria Central de Contratos e Congêneres do TJCE, no prazo máximo de um mês, contados a partir da data de homologação da licitação e anterior à assinatura do contrato, garantia da contratação no valor correspondente a 5% (cinco por cento) do valor anual do contrato, na forma do art. 96 da Lei 14.133/2021.

14.1 **VIGÊNCIA ESTENDIDA DA GARANTIA** – Esta garantia deverá valer por todo o período de vigência do contrato e por mais 03 (três) meses após o término dela e, havendo aditamento de prazo e/ou valor, a CONTRATADA deverá apresentar garantia adicional, nas mesmas condições e proporção do aditamento, de forma a atender ao novo prazo/valor contratado adicionado da extensão prevista neste, no prazo de até 10 (dez) dias úteis após a assinatura do respectivo aditivo.

14.2 COBERTURA OBRIGATÓRIA – Não será admitida a existência de cláusulas que restrinjam ou atenuem a responsabilidade do segurador ou fiador, no caso de seguro-garantia ou fiança bancária, que deve comportar necessariamente a cobertura de:

14.2.1 prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

14.2.2 prejuízos causados ao **TJCE** ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

14.2.3 multas moratórias e punitivas aplicadas pelo **TJCE** à **CONTRATADA**;

14.2.4 obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela **CONTRATADA.**

14.3 COMPLEMENTAÇÃO DA GARANTIA – Caso a garantia, ou parte dela, seja utilizada em pagamento de qualquer obrigação, inclusive multas contratuais ou indenizações a terceiros, a **CONTRATADA** obriga-se a complementá-la, no valor correspondente ao efetivamente utilizado, no prazo máximo de 10 (dez) dias úteis, contado da data em que for notificada pelo TJCE;

14.4 IRREGULARIDADE NA GARANTIA – O retardamento, a falta da apresentação, complementação ou a não substituição da garantia, além de consistir em possível motivo para rescisão imediata deste contrato, é causa suspensiva da sua execução e da realização de pagamentos, sem prejuízo da aplicação de sanções.

14.5 ATUALIZAÇÃO DA CAUÇÃO EM DINHEIRO – Quando apresentada em dinheiro, a garantia será devolvida atualizada monetariamente pelo INPC – Índice Nacional de Preços ao Consumidor emitido pelo IBGE.

14.6 DEVOLUÇÃO E EXTINÇÃO DA GARANTIA – São requisitos para liberação da garantia contratual o decurso do prazo acima previsto após o término do contrato.

14.6.1 Comprovação, pela **CONTRATADA**, do cumprimento integral das obrigações contratuais e a quitação de encargos correspondentes.

14.6.2 Não havendo comprovação do pagamento dos débitos trabalhistas e previdenciários no prazo que for concedido, a garantia poderá ser utilizada para o pagamento destas verbas diretamente pelo TJCE.

14.7 Apresentação, ao final do contrato, dos seguintes documentos:

14.7.1 Relatório circunstanciado da situação trabalhista de todos os empregados vinculados ao contrato, devidamente assinada pelo representante legal;

14.7.2 Termos de rescisão dos contratos de trabalho dos empregados acompanhados dos comprovantes de pagamento, e devidamente homologados (caso exigível por norma trabalhista aplicável); e

14.7.3 Declaração de não demissão e realocação dos empregados porventura não demitidos

14.8 NATUREZA DA GARANTIA – A garantia prevista nesta cláusula não se confunde, nem exclui ou substitui as garantias legais e técnicas porventura incidentes sobre o objeto da contratação.

CLÁUSULA DÉCIMA QUINTA – PROTEÇÃO DE DADOS PESSOAIS

15. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução

contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contratual.

15.1. O **TJCE** e a **CONTRATADA** se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, garantindo que:

15.1.1. O tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos arts. 7° e/ou 11 c/c 23 da Lei 13.709/2018;

15.1.2. O tratamento seja limitado às atividades necessárias ao atingimento das finalidades de execução do contrato, utilizando-os, quando seja o caso, em cumprimento de obrigação legal ou regulatória, no exercício regular de direito, por determinação judicial ou por requisição da ANPD;

15.1.3. Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sejam eles sensíveis ou não, a **CONTRATADA** interromperá o tratamento dos Dados Pessoais disponibilizados pelo O TJCE e, em no máximo (30) dias, sob instruções e na medida do determinado pelo O TJCE, eliminará completamente os Dados Pessoais e todas as cópias porventura existentes (seja em formato digital ou físico), salvo quando a **CONTRATADA** tenha que manter os dados para cumprimento de obrigação legal ou outra hipótese da LGPD.

15.2. As partes responderão administrativa e judicialmente na hipótese de causarem danos patrimoniais, morais, individuais ou coletivos aos titulares de dados pessoais repassados em decorrência da execução contratual, por inobservância à Lei Geral de Proteção de Dados.

15.2.1. O eventual acesso, pela **CONTRATADA**, às bases de dados que contenham ou possam conter dados pessoais implicará para a **CONTRATADA** e para seus prepostos – devida e formalmente instruídos nesse sentido – o mais absoluto dever de sigilo, no curso do presente contrato e pelo prazo de até 10 anos contados de seu termo final.

15.2.2. A **CONTRATADA** declara que se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais repassados pelo **TJCE**.

15.3. No prazo de até 24 (vinte e quatro) horas da ocorrência, a **CONTRATADA** fica obrigada a informar ao O **TJCE** qualquer incidente que implique violação ou risco de violação de dados pessoais, inclusive acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, de modo a possibilitar a adoção das providências devidas, dispostas no art. 48 da Lei Geral de Proteção de Dados, bem como o atendimento de questionamentos das autoridades competentes.

CLÁUSULA DÉCIMA SEXTA – RESPONSABILIDADES – ANTICORRUPÇÃO

16. Em demonstração de responsabilidade e comprometimento ético, a **CONTRATADA** declara, através da assinatura do presente contrato:

16.1. Conhecer e concordar integralmente com o que dispõe a legislação sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a Administração Pública, pelo que se comprometem a zelar por esta;

16.2. Que seus diretores, executivos ou empregados não ofereceram, prometeram, deram, autorizaram, solicitaram ou aceitaram qualquer valor pecuniário indevido ou outra vantagem, de qualquer tipo, e evitarão atos desta natureza relacionados ao presente contrato e tomaram as medidas necessárias para estender estas precauções aos seus representantes e empregados e prevenir subcontratados, agentes ou terceiros;

16.3. Que não vão oferecer, dar ou se comprometer a dar, a quem quer que seja, ou aceitar ou se comprometer a aceitar, de quem quer que seja, tanto por conta própria quanto através de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios, de quaisquer espécies, relacionado às execuções ou faturamentos deste contrato, garantindo que seus prepostos, empregados e subcontratados ajam da mesma forma;

16.4. Que não visam a obtenção de vantagens ou benefícios indevidos oriundos de modificações ou prorrogações deste contrato, nem pretendem dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos;

16.5. Que se comprometem em, na hipótese de indícios de descumprimento dos deveres estipulados nesta cláusula ou violação ao que dispõe a legislação, promover e colaborar com procedimento administrativo para apurar as responsabilidades;

16.6. Concordam que, se constatada qualquer prática contrária aos deveres estipulados nesta cláusula e na legislação, a infratora será responsabilizada objetivamente, nos âmbitos administrativo e civil, pelos atos lesivos praticados, não excluindo a responsabilidade individual de seus dirigentes ou administradores ou de qualquer pessoa natural, autora, coautora ou partícipe do ato ilícito, na medida da sua culpabilidade;

16.7. Na esfera administrativa, será aplicada à **CONTRATADA** responsável pelos atos lesivos – configurados por qualquer ato de empregado, dirigente ou preposto, mesmo em caso de infração desta cláusula que não tenha gerado prejuízo – previstos nesta cláusula a sanção de multa, no valor de 0,1% (um décimo por cento) a 20% (vinte por cento) do faturamento bruto do último exercício anterior ao da instauração do processo administrativo, excluídos os tributos, a qual nunca será inferior à vantagem auferida, quando for possível sua estimação, bem como publicação extraordinária da decisão condenatória;

16.8. A aplicação das sanções não exclui, em qualquer hipótese, a obrigação da reparação integral do dano causado e demais cominações previstas neste contrato.

CLÁUSULA DÉCIMA SÉTIMA - GESTÃO E FISCALIZAÇÃO DO CONTRATO

17. A execução do contrato será acompanhada por representantes do **TJCE**, definidos como Gestor e Fiscal(is) do Contrato, que manterão comunicação com o representante indicado pela **CONTRATADA**, seguindo as orientações definidas no **item 7 do Anexo 1 do Edital (Termo de Referência).**

CLÁUSULA DÉCIMA OITAVA – DAS DISPOSIÇÕES GERAIS

18. Adicionalmente às cláusulas acima estipuladas, incorporam a este contrato as seguintes disposições:

18.1 **MANUTENÇÃO E EXTENSÃO DE OBRIGAÇÕES –** este contrato é firmado em caráter irrevogável e irretratável, mantendo a **CONTRATADA** todas as obrigações contidas neste instrumento mesmo em caso de agregação de outros executores ou subcontratação, obrigando-se as partes por si e seus sucessores.

18.2 **PREVALÊNCIA DOS TERMOS CONTRATUAIS –** Os termos do presente contrato representam o fiel e completo ajuste entre as partes, prevalecendo sobre quaisquer entendimentos, formais ou informais, anteriores ou baseados nos seus anexos.

18.3 **FORMA DE COMUNICAÇÃO –** As comunicações relativas ao presente contrato de fatos ou definições que não tenham participado ambas as partes, deverão ser feitas por escrito, preferencialmente de forma eletrônica, e encaminhadas diretamente aos representantes legais da outra parte, prepostos, fiscais ou gestores previamente informados por escrito.

18.4 **POSSIBILIDADE DE SUSPENSÃO –** Em qualquer caso de identificação pelo **TJCE** de anomalia de desenvolvimento da obra ou perda de performance ou qualquer tipo de dúvida em relação ao objeto, assim como identificação de surgimento ou crescimento de situação de risco, poderá o **TJCE** suspender o presente contrato pelo prazo de até 30 (trinta) dias em razão de cada anomalia ou risco identificado, não gerando à **CONTRATADA** direito à indenização ou compensação pelo período suspenso.

18.5 **TOLERÂNCIA E NOVAÇÃO –** Qualquer tolerância de uma das partes na exigência do cumprimento do presente contrato não constituirá novação, renúncia tácita ou extinção da respectiva obrigação, podendo a mesmo ser exigida a qualquer tempo.

CLÁUSULA DÉCIMA NONA – DOS ANEXOS

19. Os documentos abaixo ficam fazendo parte do presente contrato, obrigando-se as partes a observarem e promoverem seu atendimento, porém não prevalecerão sobre suas Cláusulas expressas deste instrumento contratual:

19.1 Anexo I (Modelo Termo de Compromisso de Sigilo e Normas de Segurança);

19.2 Anexo II (Proposta da Contratada);

19.3 Anexo III (Ficha de dados do Representante legal);

19.4 Anexo IV (Termo de Nomeação de Preposto);

19.5 Anexo V (Especificações Técnicas)

19.6 Anexo VI (Termo de Ciência)

19.7 Além dos documentos acima, são partes integrantes do presente contrato o processo que originou esta contratação, incluindo proposta da **CONTRATADA** e demais documentos que acompanharam a licitação.

CLÁUSULA VIGÉSIMA – DO FORO

20. As partes elegem o Foro da Comarca de Fortaleza, capital do Estado do Ceará, que será o competente para dirimir eventuais conflitos acerca deste contrato, com renúncia a qualquer outro, por mais privilegiado que seja.

E assim, após lerem e concordarem, as partes assinam este contrato em via única eletrônica, para que surta seus efeitos jurídicos.

Fortaleza/CE, DATA DA ÚLTIMA ASSINATURA REGISTRADA PELO SISTEMA.

HERACLITO VIEIRA DE SOUSA NETO:200458
Assinado de forma digital por HERACLITO VIEIRA DE SOUSA NETO:200458
Dados: 2026.11.03 14:48:47 -03'00'

DESEMBARGADOR HERÁCLITO VIEIRA DE SOUSA NETO
PRESIDENTE DO TJCE

DENISE MARIA NOROES OLSEN:24667
Assinado de forma digital por DENISE MARIA NOROES OLSEN:24667
Dados: 2026.11.03 10:05:22 -03'00'

DENISE MARIA NORÕES OLSEN
SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO

Assinado de forma digital por LEANDRO MANOEL APARICIO:21440693870
Dados: 2026.11.04 14:24:04 -03'00'

LEANDRO MANOEL APARÍCIO
REPRESENTANTE DA EMPRESA ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA.

ANEXO I DO CONTRATO

MODELO TERMO DE COMPROMISSO DE SIGILO E NORMAS DE SEGURANÇA

TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

O TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, situado no Centro Administrativo Governador Virgílio Távora, com sede na Avenida General Afonso Albuquerque Lima, S/N, Bairro Cambeba, Fortaleza – CE, inscrito no CNPJ sob o número 09.444.530/0001-01, doravante denominado simplesmente de TJCE ou O TJCE, neste ato representado por sua(seu) Presidente, Des(a). _____ e por seu(sua) Secretário(a) de Administração e Infraestrutura, _____, e a empresa _____, representada neste ato por _____, portador da carteira de identidade n._____/___, CPF n. _____, com endereço na _____, inscrita no CNPJ sob o número _____, daqui por diante simplesmente denominada **CONTRATADA**.

CONSIDERANDO que, em razão do contrato N. º __/____ doravante denominado contrato PRINCIPAL, a **CONTRATADA** poderá ter acesso a informações sigilosas do O TJCE;

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 O TJCE;

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 sensíveis e sigilosas, disponibilizadas pelo **TJCE**, por força dos procedimentos necessários para a execução do objeto do contrato principal celebrado entre as partes e em acordo com o que dispõe o Decreto n. 7.845/2012 – Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pelo TJCE.

Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômicos, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

A **CONTRATADA** declara sob as penas da Lei, ter tomado conhecimento do TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO (TCMS), emitido por ocasião da assinatura do contrato nº _____/20__, e se compromete a seguir, naquilo que lhe couber, todas as disposições do referido Termo.

Local e data

_____

Assinatura

ANEXO II - DO CONTRATO

PROPOSTA DA CONTRATADA

TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ

PROPOSTA COMERCIAL

Ao
TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ
Ref. Pregão Nº 032/2026
Processo Nº 8515550-95.2025.8.06.0000

Objeto: Contratação de 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, quantitativos e exigências estabelecidas neste edital e seus anexos.

Dados da Contratada:

Razão Social: Add Value Participações Comércio e Serviços de Informática Ltda
CNPJ/MF: 10.864.910/0001-76
Inscrição Estadual: 206.646.758.111
Inscrição Municipal: 5.AA747-9
Endereço: Av. Marcos Penteado de Ulhoa Rodrigues, 939 Edifício Jacarandá Sala 882 | CEP: 06460-040
Cidade: Barueri UF: São Paulo
Banco: Itaú (341) Agência n.º: 0368 C/C n.º: 05041-5
Telefone: 11 4130-9832 | E-mail: ***edital@addvalue.com.br*** | Website: www.addvalue.com.br

Representante Legal:

Nome Completo: Leandro Manoel Aparício
Carteira Identidade nº: [redacted]
CPF: [redacted]
Naturalidade: São Paulo
E-mail: leandro.aparicio@addvalue.com.br

Em atendimento ao Edital do Pregão em epígrafe, apresentamos a proposta de preços:

LOTE 2					
ITEM	**BEM / SERVIÇO**	**UNIDADE**	**QUANT.**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	**Web Application Firewall (WAF) em modelo Software como Serviço (SaaS), com franquia mensal de 50TB de tráfego inspecionado**	**MÊS**	36	R$65.291,60	R$2.350.497,60
2	**Franquia adicional de tráfego inspecionado a ser consumido e contratado sob demanda durante a vigência contratual**	**TB**	900	R$433,82	R$390.438,00
3	**Proteção DNS para 1 zona**	**MÊS**	36	R$946,20	R$34.063,20
VALOR TOTAL - LOTE 2				**R$2.774.998,80**	
VALOR TOTAL DA PROPOSTA				**R$2.774.998,80 (Dois milhões, setecentos e setenta e quatro mil, novecentos e noventa e oito reais e oitenta centavos)**	

Declaramos que todos os serviços descritos e especififcados no Termo de Refrência estão contemplados nesta proposta.

Declaramos que a empresa possui todos os requisitos exigidos no edital e no termo de referência para o cumprimento do objeto contratual.

Declaramos que a presente proposta econômica compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

Ao efetuar essa proposta, esta empresa proponente declara ter tomado pleno conhecimento do Edital, do Termo de Referência e dos demais documentos integrantes da presente licitação, bem como das informações e condições locais, estando ciente das obrigações das partes e das condições de prestação dos serviços, para o cumprimento das obrigações objeto dessa licitação.

Esta empresa proponente declara que que nos preços cotados estão inclusas todas as despesas, tais como custos diretos e indiretos, inclusive os resultantes da incidência de quaisquer impostos, taxas, contribuições ou obrigações trabalhistas, fiscais, previdenciárias, transporte em veículos apropriados, seguros, embalagens, certificações, instalação ou adequação elétrica, bem como a instalação de equipamentos, configuração ou quaisquer outros encargos decorrentes do exercício profissional de seus funcionários ou terceirizados e outros gravames que possam incidir sobre o objeto licitado.

O prazo de validade desta proposta é de 90 (noventa) dias corridos.

Pagamento: Conforme definido no Termo de Referência.

Prazo de Entrega: Conforme definido no Termo de Referência.

São Paulo, 08 de Setembro de 2026.

Assinado de forma digital por LEANDRO MANOEL APARICIO:21440693870
Dados: 2026.09.08 17:52:08 -03'00'

REPRESENTANTE LEGAL DA EMPRESA
Leandro Manoel Aparício
CPF: [redacted]
CFO

ANEXO III DO CONTRATO

FICHA DE DADOS DO REPRESENTANTE LEGAL

Dados pessoais do(s) representante(s) e/ou procurador(es), devidamente habilitados, da futura CONTRATADA, indicado(s) para assinatura do Termo de Contrato:

NOME	:	Leandro Manoel Aparício
NACIONALIDADE	:	
ESTADO CIVIL	:	
PROFISSÃO	:	
RG	:	
CPF	:	214.XXX.XXX-70
DOMICÍLIO	:	Av. Marcos Penteado de Ulhoa Rodrigues, 939
CIDADE		São Paulo
UF	:	SP
FONE	:	(11) 4130-9832
CELULAR	:	
E-MAIL	:	leandro.aparicio@addvalue.com.br

ANEXO IV DO CONTRATO

TERMO DE NOMEAÇÃO DE PREPOSTO

CONTRATO/ INSTRUMENTO EQUIVALENTE Nº	XXXX		
OBJETO DA DEMANDA	XXXX		
FORNECEDORA	XXXX	**CNPJ**	XX.XXX.XXX/XXXX-XX

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)

ANEXO V DO CONTRATO

ESPECIFICAÇÕES TÉCNICAS

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 retornar 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:48994

Assinado de forma digital por MAX EDUARDO VIZCARRA MELGAR:48994
Dados: 2026.07.16 15:29:22 -03'00'

Max Eduardo Vizcarra Melgar
Integrante Técnico

ANEXO VI DO CONTRATO

TERMO DE CIÊNCIA

ANEXO V – TERMO DE CIÊNCIA

AQSETIN2025003 – Solução de balanceamento de carga e WAF

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