



ANEXO I – TERMO DE REFERÊNCIA

Contratação de Registro de Preço de 04 (quatro) Appliances Virtuais WAF

1 OBJETO

1.1 Definição

Constitui objeto da presente licitação o registro de preço para futura e eventual aquisição de 04 (quatro) appliances virtuais de firewall de aplicações web (WAF – Web Firewall Application), incluindo serviço de implantação da solução e serviços continuados de garantia, licenciamento, suporte e gerenciamento, atendendo às condições deste Edital e seus Anexos.

2 FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1 Motivação

A unidade demandante, COTEC, visando a segurança das informações internas e das de propriedade dos cidadãos sob a custódia do Poder Judiciário, deseja contratar uma solução de Web Application Firewall para analisar e proteger de ameaças que estão além da capacidade dos firewalls tradicionais, criando uma barreira entre serviço baseado na web e as principais ameaças.

Esta contratação está alinhada com uma série de normas destacando-se, dentre estas, a Lei Geral de Proteção de Dados Pessoais, Lei 13.709/2018, que entrará em vigor em 2020 visando proteger as informações privadas dos cidadãos brasileiros.

A LGPD estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção e penalidades para o não cumprimento. Quando essa legislação entrar em vigor, as empresas só poderão coletar dados pessoais com o consentimento do titular, sendo obrigadas a deixar claro o motivo da coleta dessas informações e como serão tratadas. Além disso, o usuário deverá ter acesso fácil a tais dados, podendo revogar o uso dos mesmos a qualquer momento. Questões mais sensíveis, como religião, posição política ou orientação sexual serão tratados com ainda mais rigor.

As tecnologias também serão componentes importantes para as organizações, uma vez que a nova lei traz desafios de gestão e governança de privacidade, tais como a gestão de consentimentos (e respectivas revogações), gestão das petições abertas por titulares (que, em alguns casos, devem ser respondidas imediatamente), gestão do ciclo de vida dos dados pessoais (data mapping & data discovery) e implementação de técnicas de anonimização (os dados anonimizados não serão considerados dados pessoais pela lei desde que o processo não seja reversível).

De forma geral, os órgãos, autarquias e secretarias dos poderes legislativo, executivo e judiciário precisarão estar em conformidade com esta lei, no máximo, até o mês de agosto de 2020, o que motiva a abertura deste processo licitatório, levando em consideração a contratação das soluções e a maturação do processo, até sua fase de implementação, capacitação e conclusão.

Para o atendimento imediato da demanda existente, inicialmente serão instalados 02 (dois) Appliances virtuais na sala cofre localizada no edifício sede do Tribunal de Justiça da Bahia, que atualmente hospeda todas as aplicações web utilizados pelos Servidores e Magistrados do TJBA, bem como a órgãos parceiros e toda a população que faz uso dos serviços e sistemas disponibilizados por este Tribunal.

Contudo, a sala cofre está muito próxima de seu limite físico no que se refere a questões de carga elétrica e de refrigeração, de modo que o TJBA está em avançado processo (TJ-ADM-2020/29805) para contratação de serviço de nuvem pública para ampliar e suportar a demanda crescente de Infraestrutura para hospedar suas aplicações.

Prevendo essa expansão potencial de aplicações para ambiente de nuvem pública, sugere-se realizar um registro de preços, adicionando mais 02 (dois) virtuais appliances de Web Application Firewall (WAF), possibilitando dispor dos mesmos itens de segurança neste novo ambiente de Cloud que possui contratação estimada de acontecer em dentro da vigência desta ATA.



2.2 Objetivos

- 2.2.1 Aprimorar e expandir os recursos de Segurança da Informação em uso no Poder Judiciário do Estado da Bahia.
- 2.2.2 Implementar os controles necessários para atender as exigências da Lei de Acesso à Informação, Marco Civil da Internet e Lei Geral de Proteção de Dados Pessoais, bem como à Política de Segurança da Informação do TJBA.
- 2.2.3 Garantir à disponibilidade da solução que fornece proteção contra ataques virtuais;
- 2.2.4 Alta disponibilidade e integridade do ambiente tecnológico deste Tribunal
- 2.2.5 Manter as aplicações web mais seguras, com a implementação de regras personalizadas, minimizando os problemas relacionados, tais como:
 - . Injeção de dados;
 - . Exposição de dados confidenciais;
 - . Quebra de sessão e gerenciamento de sessões.

2.3 Benefícios

- 2.3.1 Garantir a disponibilidade da rede de computadores do Poder Judiciário.
- 2.3.2 Garantir a disponibilidade de sistemas essenciais de Tecnologia da Informação e Comunicação.
- 2.3.3 Garantir a confidencialidade dos processos sigilosos.
- 2.3.4 Aprimorar a prestação jurisdicional.
- 2.3.5 Contribuir com a imagem institucional do Poder Judiciário.

2.4 Alinhamento Estratégico

O presente processo está alinhado ao item 15 do Planejamento Estratégico do Poder Judiciário do Estado da Bahia para o período de 2015 – 2020: “Perspectiva dos Recursos”, macrodesafio “Melhoria da Infraestrutura e da TIC”, nos seguintes objetivos:

- . Garantir a disponibilidade de sistemas essenciais de Tecnologia da Informação e Comunicação.
- . Garantir a infraestrutura de TIC apropriada e segura às atividades judiciais, extrajudiciais e administrativas.

Atende, ainda, à Lei Geral de Proteção de Dados Pessoais, Lei 13.709/2018, e à Política de Segurança da Informação do TJBA, que institui normas para utilização de recursos de tecnologia da informação, gestão de ativos, classificação de informações, gerenciamento de acessos, gestão operacional, desenvolvimento seguro e gerenciamento de riscos, no âmbito da Tecnologia da Informação do Poder Judiciário do Estado da Bahia.

Esta demanda está prevista no Plano de Contratações de STIC – exercício de 2020, da SETIM/TJBA, em observância à Resolução nº182/2013, Art. 7º, § 4º. Neste plano de contratações consta como: Serviços de suporte e ampliação da infraestrutura de proteção de dados.

2.5 Referência aos Estudos Preliminares

Este Termo de Referência foi elaborado com base nas informações contidas no Documento de Oficialização da Demanda (DOD) encaminhado pela Coordenação Técnica (COTEC) para a Secretaria de Tecnologia da Informação e Modernização (SETIM) e no conteúdo dos Estudos Preliminares desenvolvidos pela equipe de planejamento da contratação. Todos os documentos encontram-se no Processo Administrativo TJ-ADM-2020/19040 de que trata esta contratação, em tramitação no SIGA.

2.6 Relação entre a Demanda Prevista e a Contratada

A demanda é de caráter permanente. Sendo a contratação bem-sucedida, ela será atendida em forma contínua durante 38 (trinta e oito) meses.

Tendo em vista o atendimento imediato da demanda existente, inicialmente serão instalados 02 (dois) Appliances virtuais com a forma de instalação estabelecida no Tópico 3.3 – Dinâmica da Execução.



2.7 Análise de Mercado de TIC

2.7.1 Soluções Contratadas por Outros Órgãos

Dentre as contratações públicas similares, foram especialmente analisados os seguintes processos licitatórios:

2.7.1.1 Banco Central do Brasil – Ministério da Economia

Resumo: Expansão da Solução de Balanceamento de Carga do fabricante F5, incluindo suporte e operação assistida. A SOLUÇÃO DE BALANCEAMENTO deverá ser composta dos seguintes elementos: 8 appliances virtuais especializados em serviços de balanceamento e firewall de aplicação; 4 appliances virtuais especializados em DNS; 1 appliance virtual para o gerenciamento de todos os demais elementos. A solução de Balanceamento no BCB deverá estar equipada com todos os elementos necessários ao seu perfeito funcionamento (softwares e licenças), permitindo acesso aos serviços de redes providos pelo BCB de acordo com as funcionalidades definidas nesse projeto. Caso a LICITANTE necessite fornecer softwares adicionais não especificados nominalmente neste Edital, mas necessários para atender as funcionalidades exigidas, o custo desses deverão estar inseridos no preço total ofertado Valor: **R\$ 2.400.000,00**. Homologado em : 14/05/2020.

2.7.1.2 COGEL – Prefeitura de Salvador Bahia

Resumo: Contratação, em lote único, na modalidade de Registro de Preços, de empresa especializada em Tecnologia da Informação e Comunicação – TIC para aquisição de solução de Firewall de Aplicações Web (WAF) e de Gateway de Segurança de E-mail, englobando o fornecimento de todo hardware, software, subscrições, instalação, configuração, suporte técnico, treinamento, manutenção remota e local com reposição de peças, visando futuras contratações. Composto dos seguintes itens: 1 Solução de Firewall de Aplicação Web (WAF), 1 Ampliação de Performance da Solução de Firewall de Aplicação Web (WAF), 1 Solução de Gateway de Segurança de E-mail, 1 Ampliação de Performance da Solução de Gateway de Segurança de E-mail – Nível 1 e 1 Ampliação de Performance da Solução de Gateway de Segurança de E-mail – Nível 2. Registro homologado no DOM de 18 de Setembro de 2019

2.7.2 Definição e Justificativa da Solução Adotada

A ampla e intensa utilização da Tecnologia da Informação – TI, tanto em nível estratégico como operacional, é uma realidade nas organizações de todos os portes. Neste sentido, a Segurança da Informação se torna elemento indispensável à estratégia das instituições, uma vez que, os benefícios proporcionados pela TI são acompanhados por ameaças que podem comprometer a confidencialidade, integridade e disponibilidade das informações.

Com a contínua evolução da tecnologia, as aplicações corporativas e a infraestrutura necessária para suportá-las se tornam cada vez mais complexas e indispensáveis. Em se tratando de segurança da informação, testemunhamos o crescimento tanto no número como no nível de sofisticação dos crimes virtuais, principalmente àqueles causados por códigos maliciosos comumente chamados de vírus. Os impactos decorrentes desses ataques podem comprometer a área de TI, assim como a outros setores da organização, podendo causar prejuízos financeiros, interrupção de serviços críticos, perda de propriedade intelectual, vazamento de informações confidenciais, danos à imagem e reputação organizacional, dentre outros.

Diante de tantas ameaças e incidentes cibernéticos, as disciplinas (legislações) que estudam os reflexos jurídicos das inovações tecnológicas focadas em garantir a privacidade e a segurança de informações online precisaram se reorganizar. Uma série de medidas foram e estão sendo tomadas a fim de abonar a proteção ao mundo virtual. Dentre elas, destacam-se:

- Política de Segurança do Tribunal de Justiça do Estado da Bahia – Decreto nº 474/2019;
- Lei de Acesso à Informação – nº 12.527/2011;
- Marco Civil da Internet – nº 12.965/2014;
- Lei Geral de Proteção de Dados – LGPD nº 13.709/2018

Neste contexto, o TJBA, visando à segurança das suas informações e as de propriedade dos cidadãos sob a sua custódia, pretende contratar um de soluções de Segurança da Informação que proteja de maneira eficiente o parque computacional e viabilize a implementação de medidas alinhadas às normas supracitadas, com o objetivo de reduzir a superfície de ataques, detectar e bloquear códigos e atividades maliciosas, assim como mitigar os seus impactos.



2.8 Natureza do Objeto

Trata-se da aquisição de appliance virtual com os serviços para sua operacionalização de natureza comum.

2.8.1 Vigência do Contrato

Este contrato terá vigência de 38 (trinta e oito) meses podendo a vigência dos serviços se estender por mais de um exercício financeiro, renovando até o limite legal de tempo.

A partir do primeiro aditamento, a renovação será realizada para o licenciamento e suporte/gerenciamento continuado e terá como base o valor mensal estabelecido nos itens 2 e 4 da Proposta Comercial.

2.9 Parcelamento e Adjudicação do Objeto

Tendo em vista a peculiaridade deste tipo de solução, mantendo a sua integridade e inviolabilidade, não é indicado um parcelamento deste objeto.

Como não está indicado o parcelamento, o objeto deverá ser adjudicado a um único fornecedor.

2.10 Modalidade, Tipo de Licitação e Critérios de Aceitabilidade da Proposta

Considerando tratar-se de serviço comum, será utilizada a modalidade Pregão Eletrônico com seleção da melhor proposta pelo menor preço global.

2.10.1 Limites Máximos de Preço

Conforme as referências constantes nos Estudos Preliminares, as quais levaram em conta tanto as especificidades dos serviços objeto desta contratação quanto a realidade de seu atendimento pelo mercado, com respaldo da Consultoria Jurídica da Presidência do TJBA e do acórdão 1850/2020, do Plenário do TCU, os limites máximos de preços aceitáveis para cada item são dados pela tabela a seguir:

Item	Descrição	Quantidade Registrada	Num Parcelas	Valor Unitário	Valor MÁXIMO para o Item
1.	Virtual Appliance com garantia de 36 meses Marca/ Modelo/Versão:	4	1 (uma)	R\$426.128,24	R\$1.704.512,96
2.	Licenciamento da solução, suporte e atualizações do fabricante por 36 meses.	4	36 (trinta e seis) meses consecutivos	R\$20.114,88	R\$2.896.542,00
3.	Serviço de Implantação da solução e configuração de aplicações protegidas.	2	1 (uma)	R\$235.000,00	R\$470.000,00
4.	Serviço de Suporte da solução com Gerenciamento Continuado por 36 meses.	2	36 (trinta e seis) meses consecutivos	R\$14.812,50	R\$1.066.500,00
Limite máximo de preço aceitável para contratação					R\$6.137.554,96

Não serão aceitas propostas cujo valor global esteja dentro do limite máximo, mas não estejam cumprindo o limite máximo do item.

O valor máximo referencial para esta contratação é de **R\$6.137.554,96** (Seis milhões, cento e trinta e sete mil, quinhentos e cinquenta e quatro reais e noventa e seis centavos) e todas e quaisquer despesas necessárias ao cumprimento do objeto desta licitação, tais como mão de obra, impostos, tributos, encargos e contribuições sociais, fiscais, parafiscais, fretes, seguros, transporte, estadia, alimentação e demais despesas inerentes, correrão por conta da CONTRATADA, não cabendo ao CONTRATANTE o reembolso de despesas com transporte, hospedagem e outros custos operacionais, não previstos neste termo de referência, que devem ser de exclusiva responsabilidade da CONTRATADA.



2.10.2 Habilitação e Qualificação Técnica

Para fins de habilitação técnica, a licitante arrematante deve, na forma e nos prazos indicados no edital, atender aos seguintes aspectos:

- 2.10.2.1 Comprovação de parceria com o fabricante da solução ofertada emitida pelo fabricante da solução.
 - 2.10.2.2 Uma tabela indicando a comprovação de todas as funcionalidades apresentadas no **Tópico 4 – Requisitos Técnicos Específicos**.
 - 2.10.2.3 Entregar atestado(s) de capacidade técnica, expedido(s) por pessoa jurídica de direito público ou privado, que comprove(m) que a arrematante tenha executado, ou esteja executando o serviço, comprovando atividade pertinente e compatível, em quantidades, prazos e as características técnicas/operacionais do lote. Para comprovar suficientemente a aptidão da empresa licitante, os atestados deverão conter informações detalhadas sobre os serviços prestados, tais como nome dos itens de software fornecidos, quantidade de sites protegidos, tempo de execução efetiva dos serviços associados e grau de satisfação do CONTRATANTE. Caso o nome do produto ou software tenha sido alterado pelo fabricante, deverá ser apresentado documento oficial do fabricante comprovando esta alteração.
 - 2.10.2.4 Para os atestados emitidos por empresa da iniciativa privada, não serão acolhidos aqueles emitidos por empresa pertencente ao mesmo grupo empresarial da licitante, sua subsidiária, controlada ou controladora e por empresa na qual haja pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da arrematante.
 - 2.10.2.5 Somente serão aceitos atestados referentes a contratos já encerrados ou referentes a contratos cuja execução já tenha alcançado pelo menos 50% do volume de seu respectivo objeto, no que concerne aos serviços que se pretende atestar.
 - 2.10.2.6 É preferível que os atestados emitidos por pessoa jurídica de direito privado contenham assinatura digital certificada ou com reconhecimento de firma, que assegure sua autenticidade. Caso a assinatura do responsável técnico não contenha elemento de autenticação, a Contratante se resguarda ao direito de realizar diligência para solicitar documentos a fim de sanar eventuais dúvidas quanto ao referido atestado.
 - 2.10.2.7 O Tribunal de Justiça do Estado da Bahia se reserva o direito de realizar diligências para averiguar a veracidade dos documentos e declarações, junto à pessoa jurídica emissora dos Atestados e/ou Declaração, visando obter informação sobre o serviço prestado e cópias dos respectivos contratos e aditivos e/ou outros documentos comprobatórios do conteúdo declarado. Quando solicitado através de diligência, o licitante deverá prontamente disponibilizar todas as informações necessárias à comprovação da legitimidade dos respectivos atestados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, sob pena de inabilitação.
- 2.10.3 Será admitida a Subcontratação, não se responsabilizando o CONTRATANTE por nenhum compromisso assumido pela CONTRATADA com a(s) SUBCONTRATADA(S). Para tanto, deverão ser respeitados os seguintes requisitos:
- 2.10.3.1 Só será permitido à CONTRATADA a subcontratação dos seguintes tópicos desta prestação de serviço:
 - 2.10.3.1.1 – Instalação da solução
 - 2.10.3.1.2 – Atividades presenciais pós-implantação.
 - 2.10.3.2 Na eventualidade de subcontratação a mesma deverá ser submetida à prévia consulta e autorização escrita do CONTRATANTE, devendo preferencialmente ser subcontratadas, micro ou pequenas empresas, em consonância à Lei Complementar nº 123/06, alterada pela Lei Complementar nº 128/08, sem subordinação e pessoalidade com o CONTRATANTE.
 - 2.10.3.3 Na hipótese de ser autorizada a subcontratação, a CONTRATADA diligenciará junto a esta no sentido de serem rigorosamente cumpridas às obrigações contratuais, especialmente quanto à fiel e perfeita execução dos serviços subcontratados, ficando diretamente responsável, perante o CONTRATANTE, pelas obrigações assumidas pela subcontratada.



- 2.10.3.4 A CONTRATADA formalizará com a subcontratada o instrumento contratual de subcontratação, o qual deverá ser submetido à apreciação da Administração do CONTRATANTE, que, caso decida pela aprovação, concederá autorização através do termo preenchido conforme modelo do **ANEXO III – Termo de Aceitação e Autorização Expressa de Subcontratação**. Após assinaturas ao termo, será ressaltada à CONTRATADA as novas responsabilidades surgidas da admissão da nova subcontratada, bem como inclusão da subcontratada no rol de fiscalização rotineira de contratos do CONTRATANTE.
- 2.10.3.5 A qualquer momento o CONTRATANTE poderá solicitar à CONTRATADA a apresentação dos comprovantes dos pagamentos realizados por meio da subcontratação, documentação que comprove sua habilitação jurídica, regularidade fiscal e qualificação técnica.
- 2.10.3.6 A operacionalização da subcontratação respeitará a seguinte sequência de procedimentos:
- 2.10.3.6.1 Solicitação escrita da CONTRATADA para o Gestor do Contrato indicando:
- 2.10.3.6.1.1 Parcela a subcontratar conforme normatizado pelo tópico 2.10.3.1.
- 2.10.3.6.1.2 Qualificação da prestadora de serviços que se pretende subcontratar, que deverá comprovar perante o CONTRATANTE que está em situação regular fiscal e previdenciária e que entre seus diretores ou sócios não constem funcionários, empregados ou ocupantes de cargo comissionado do órgão contratante.
- 2.10.3.6.2 Avaliação preliminar de cabimento e pertinência técnica e operacional pelo Gestor do Contrato que:
- 2.10.3.6.2.1 Denegará de plano o pleito quando encontre vedação contratual ou riscos operacionais, devolvendo o pedido à CONTRATADA constando respectiva justificativa; ou
- 2.10.3.6.2.2 Elaborará o “Termo de Aceitação e Autorização Expressa de Subcontratação”, submetendo-o à apreciação do CONTRATANTE.
- 2.10.3.7 O CONTRATANTE não aceitará, sob nenhum pretexto, a transferência de responsabilidades da CONTRATADA para outras entidades, sejam fabricantes, técnicos ou subcontratadas.
- 2.10.4 Não será admitida a participação de interessados sob a forma de consórcio.

2.11 Adequação do Ambiente

Nos locais em que a CONTRATADA execute serviços, deverão sempre ser mantidas as mesmas condições estéticas do local. Os serviços de instalação não devem obstruir o andamento das rotinas de trabalho nos ambientes objetos de intervenção. Quando houver intervenção nestes ambientes, é de responsabilidade da CONTRATADA, a recomposição total dos mesmos deixando os locais totalmente limpos e arrumados inclusive com relação a algum dano a eles causado quando da execução dos serviços.

2.12 Conformidade Técnica e Legal

- A execução dos serviços deverá respeitar, no que for pertinente, as seguintes normas:
- . Decreto Judiciário nº 474, de 16 de agosto de 2019, que regulamenta a Política de Segurança da Informação e institui Normas para Utilização de Recursos de Tecnologia da Informação, Gestão de Ativos, Classificação de Informações, Gerenciamento de Acessos, Gestão de Operação de Tecnologia da Informação, Desenvolvimento Seguro e Gerenciamento de Riscos de Tecnologia da Informação, no âmbito do Poder Judiciário do Estado da Bahia;
 - . Lei Federal nº 12.527/2011 (Lei de Acesso à Informação);
 - . Lei Federal nº 12.965/2014 (Marco Civil da Internet);
 - . Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

2.13 Obrigações da Contratada

- 2.13.1 Prestar os serviços conforme especificações, quantidades, prazos e demais condições estabelecidas no edital e seus anexos, na proposta e no contrato.



- 2.13.2 Participar de reunião de alinhamento a ser realizada em data e horário a ser definido pelo CONTRATANTE, nos termos estabelecidos do tópico - **3.4.1 Reunião de Alinhamento**.
- 2.13.3 Estar disponível para realizar reuniões periódicas com o CONTRATANTE, podendo este último, em atenção a circunstâncias específicas, dispensar reuniões programadas ou convocar, em caso de necessidade, reuniões extraordinárias, às que um representante da CONTRATADA deve comparecer no prazo máximo de dois dias úteis.
- 2.13.4 Reportar formal e imediatamente ao Gestor do Contrato do CONTRATANTE quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução dos serviços.
- 2.13.5 Seguir as instruções e observações efetuadas pelo Gestor do Contrato do CONTRATANTE, bem como reparar, corrigir, remover, reconstruir ou substituir às suas expensas, no todo ou em parte, serviços efetuados em que se verificarem vícios, defeitos ou incorreções.
- 2.13.6 Dimensionar a solução, instalar, configurar e prestar serviços continuados de garantia, suporte e atualização da solução fornecida, durante toda a vigência do contrato.
- 2.13.7 Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante toda a vigência do Contrato, dentro dos prazos e condições estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas contratualmente, caso os prazos e condições não sejam cumpridos.
- 2.13.8 Arcar com todas as despesas decorrentes de transporte e alimentação, além de assistência médica e de pronto-socorro para seus empregados envolvidos nas atividades motivo desta contratação.
- 2.13.9 Promover, por sua conta e risco, o transporte de seus empregados, materiais e utensílios necessários à execução dos serviços objeto do contrato, até as instalações do CONTRATANTE.
- 2.13.10 A CONTRATADA deverá assumir a responsabilidade por todas as providências e obrigações, estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas, os seus empregados, durante a execução desse Contrato.
- 2.13.11 A CONTRATADA deverá assumir a responsabilidade por todos os encargos, de possível demanda trabalhista, civil ou penal, relacionada à execução do Contrato, originariamente ou vinculada por prevenção, conexão ou continência.
- 2.13.12 Quando do comparecimento às dependências da CONTRATANTE, o preposto e os colaboradores da CONTRATADA deverão estar devidamente identificados com fardamento ou crachá no qual conste seu nome, o nome da empresa e a função desempenhada.
- 2.13.13 Respeitar e fazer com que seus empregados respeitem as normas de segurança do trabalho, disciplina e demais regulamentos vigentes no Poder Judiciário da Bahia, bem como atentar para as regras de cortesia no local onde serão executados os serviços objeto do contrato.
- 2.13.14 Zelar pela boa e completa execução dos serviços contratados, mantendo recursos técnicos e humanos de reserva para evitar a interrupção indesejada dos mesmos.
- 2.13.15 Além de contar com profissionais de reserva nos mesmos perfis, será obrigação da CONTRATADA cuidar de que os mesmos estejam constantemente a par das atividades em curso, evitando-se, assim, a interrupção e/ou queda na qualidade dos serviços.
- 2.13.16 Facilitar por todos os meios a seu alcance a ampla ação fiscalizadora dos prepostos designados pelo CONTRATANTE, atendendo prontamente as observações e exigências que lhe forem dirigidas.
- 2.13.17 Seguir a legislação no que tange às normas e regras para pagamento de hora extra e sobreaviso conforme o sindicato que rege os profissionais contratados.
- 2.13.18 Responder perante o CONTRATANTE pela conduta dos seus empregados designados para execução dos serviços objeto do contrato.
- 2.13.19 Responder por quaisquer prejuízos que seus profissionais causarem ao patrimônio do CONTRATANTE ou a terceiros, por ocasião da prestação dos serviços, procedendo imediatamente aos reparos ou indenizações cabíveis e assumindo o ônus decorrente.



- 2.13.20 Utilizar as melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações contidas no contrato, edital e seus anexos.
- 2.13.21 Utilizar a ferramenta de gestão de chamados de propriedade da CONTRATADA, provendo relatórios em português com base neste banco de incidentes de acordo com o período apurado, provendo informações do tipo: Incidente registrado, técnico alocado, solução adotada, data de abertura do chamado, hora de início do atendimento, data de encerramento e hora de conclusão.
- 2.13.22 Pagar os salários e encargos sociais devidos pela sua condição de única empregadora do pessoal designado para execução dos serviços contratados, incluindo indenizações decorrentes de acidentes de trabalhos, demissões, vale-transporte, entre outros, obrigando-se, ainda, ao fiel cumprimento das legislações trabalhistas e previdenciárias, sendo-lhes defeso invocar a existência deste contrato para eximir-se destas obrigações ou transferi-las para o CONTRATANTE.
- 2.13.23 Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do CONTRATANTE.
- 2.13.24 Responsabilizar-se integralmente pelos recursos técnicos e humanos, primando pela qualidade, desempenho, eficiência, disponibilidade e produtividade, visando à execução dos trabalhos durante toda a vigência do contrato, dentro dos prazos e condições estipulados, sob pena de ser considerado infração passível de aplicação de penalidades previstas contratualmente, caso os prazos e condições não sejam cumpridos.
- 2.13.25 Manter sigilo total de todos os dados ou informações a que tiver acesso, não podendo, em hipótese alguma, divulgar resultados, parciais ou totais, ou fazer qualquer comentário sobre as informações a que tenha tido acesso, o levantamento realizado e o conteúdo dos produtos gerados. Deve, ainda, adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, mesmo após o término do contrato, sob pena de responsabilidade administrativa, civil e/ou penal.
- 2.13.26 Somente divulgar quaisquer informações a que tenha acesso, em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, com autorização, por escrito, do CONTRATANTE.
- 2.13.27 Deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do Contrato, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes.
- 2.13.28 Quando da assinatura do contrato, por meio de seu representante, assinar **Termo de Confidencialidade**, conforme modelo do **ANEXO IV**, em que se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação. O termo visa assegurar que a CONTRATADA manterá sigilo, sob pena de responsabilidade cível, penal e administrativa acerca de informações consideradas como de interesse restrito ou confidencial, e não podem ser de conhecimento de terceiros, como por exemplo:
- . Programas de computador, seus códigos-fonte e códigos-objeto, bem como suas listagens e documentações.
 - . Toda a informação relacionada a programas de computador existentes ou em fase de desenvolvimento no âmbito do CONTRATANTE e rotinas desenvolvidas por terceiros, incluindo fluxogramas, estatísticas, especificações, avaliações, resultado de testes, arquivo de dados, versões “beta” de quaisquer programas, dentre outros.
 - . Documentos relativos à lista de usuários do CONTRATANTE e seus respectivos dados, armazenados sob qualquer forma.
 - . Metodologias e ferramentas de serviços, desenvolvidas pelo CONTRATANTE.
 - . Parte ou totalidade dos modelos de dados que subsidiam os sistemas de informações do CONTRATANTE, sejam eles executados interna ou externamente.



- . Parte ou totalidade dos dados ou informações armazenadas nas bases de dados que subsidiam os sistemas de informações do CONTRATANTE sejam elas residentes interna ou externamente.
 - . Circulares e comunicações internas do CONTRATANTE.
 - . Quaisquer processos ou documentos classificados como RESTRITO ou CONFIDENCIAL pelo CONTRATANTE.
- 2.13.29 O fornecedor não poderá armazenar consigo qualquer documento técnico que contemple configurações e regras de segurança aplicadas nos equipamentos implantados na rede do PJBA.
- 2.13.30 Todos os perfis de acesso e caixas postais eventualmente concedidos ao fornecedor deverão ser imediatamente excluídos após o término do contrato.
- 2.13.31 O PJBA terá propriedade sobre todos os dados, documentos e procedimentos operacionais produzidos no escopo da presente contratação.
- 2.13.32 Responsabilizar-se pela observância às Leis, Decretos, Regulamentos, Portarias e demais normas legais, direta e indiretamente aplicáveis ao contrato.
- 2.13.33 Caberá à CONTRATADA a disponibilização dos recursos necessários para prover a execução de todos os fornecimentos e serviços definidos neste Termo de Referência, além dos serviços oriundos de mudança, atualização ou evolução tecnológica que venham a ocorrer.
- 2.13.34 Caberá a CONTRATADA adequar-se ao uso das novas tecnologias e equipamentos que porventura sejam incorporados ao parque tecnológico do Poder Judiciário, inclusive treinando os seus profissionais para o desempenho de cada serviço.
- 2.13.35 A CONTRATADA deverá responsabilizar-se integralmente pela execução completa e satisfatória do fornecimento e dos serviços associados, por meio do gerenciamento dos seus recursos humanos e técnicos, assim como, não poderá se eximir dessa obrigação, ainda que parcialmente, atribuindo quaisquer falhas ou deficiências a imperícia de pessoal ou a erros de especificações.

2.14 Obrigações do Contratante

Em conformidade com as obrigações resultantes da Lei nº 9433/05, o TJBA deverá:

- 2.14.1 Designar servidores para acompanhamento e fiscalização do contrato, conforme disposto no Art. 16 da Resolução 182/2013 do Conselho Nacional de Justiça – CNJ.
- 2.14.2 Exercer a fiscalização dos serviços, podendo recusar qualquer serviço que não esteja de acordo com as condições estabelecidas neste termo.
- 2.14.3 Assegurar-se da boa prestação dos serviços, verificando sempre seu bom desempenho.
- 2.14.4 Atestar, por intermédio de servidor especialmente designado, as notas fiscais referentes aos serviços e fornecimentos prestados de forma satisfatória.
- 2.14.5 Efetuar o pagamento devido à CONTRATADA, dentro do prazo estipulado, desde que cumpridas todas as formalidades e exigências contratuais.
- 2.14.6 Zelar para que, durante a vigência do contrato, sejam cumpridas as obrigações assumidas por parte da CONTRATADA, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas.
- 2.14.7 Manter em arquivo, junto ao processo administrativo ao qual está vinculado o presente termo, toda a documentação referente ao mesmo.
- 2.14.8 Disponibilizar todas as informações necessárias para o desenvolvimento dos trabalhos.
- 2.14.9 Fornecer a infraestrutura necessária para o pleno funcionamento dos Serviços, seguindo as especificações técnicas fornecidas pela CONTRATADA e dentro das normas ABNT relacionadas. Entende-se como infraestrutura os recursos computacionais necessários para a execução da plataforma.
- 2.14.10 Validar e aprovar os serviços executados, em conformidade com as regras e requisitos estabelecidos no ANS (Acordo de Níveis de Serviço).



- 2.14.11 Providenciar o acesso controlado dos profissionais da CONTRATADA ao ambiente de TI, incluindo bibliotecas de programas, políticas, normas, procedimentos, metodologias, bases de dados, ferramentas, de acordo com pré-requisitos definidos nas comunicações formais de demanda.
- 2.14.12 Aplicar as sanções conforme previsto no contrato.
- 2.14.13 Caberá ao CONTRATANTE a gestão e fiscalização quantitativa e qualitativa da execução das demandas através do acompanhamento das atividades desenvolvidas e resultados obtidos, observando os prazos e produtos acordados com vistas a efetuar eventuais ajustes e correções de rumo.

3 DETALHAMENTO DO OBJETO

3.1 Modelo de Execução e de Gestão do Contrato

- 3.1.1 A execução do Contrato seguirá uma metodologia de trabalho baseada no conceito de Delegação de Responsabilidades. Ao CONTRATANTE caberá a definição das demandas e a gestão qualitativa dos resultados a serem obtidos por meio das atividades desenvolvidas dentro dos prazos e produtos acordados.
- 3.1.2 À CONTRATADA caberá a responsabilidade pela execução operacional dos serviços, por meio do gerenciamento dos seus recursos humanos e técnicos.
- 3.1.3 Todo e qualquer serviço somente poderá ser iniciado pela contratada após emissão de ordem de serviço formal pelo contratante, devendo obedecer rigorosamente aos requisitos a seguir.

3.2 Principais Papéis

- 3.2.1 Patrocinador da Contratação: Titular da SETIM – Secretaria de Tecnologia da Informação e Modernização, área demandante, responsável por representar os interesses do TJBA no contexto desta contratação, pela aprovação da necessidade e, por fim, pela negociação das ações necessárias para que os objetivos sejam alcançados
- 3.2.2 Gestor do Contrato: Servidor a ser oportunamente designado mediante portaria, em obediência ao Manual de Gerenciamento e Fiscalização de Contratos do Tribunal de Justiça e ao Decreto Judiciário nº 379, de 8 de maio de 2018, com as seguintes responsabilidades:
- . Planejar e orientar a contratação, especialmente para estabelecer diretrizes para a contratação e condução dos vínculos contratuais.
 - . Manter fluxo de comunicação e administrar as relações com a CONTRATADA.
 - . Acompanhar o andamento do contrato, especialmente no referente aos cumprimentos e descumprimentos contratuais.
 - . Manter-se sempre informado de todas as ocorrências contratuais e repassar às autoridades, proativamente, aquelas que interfiram no fornecimento e/ou nos serviços de garantia.
 - . Paralisar a execução do contrato no caso de estar em desacordo com o pactuado ou diante de graves descumprimentos pelo fornecedor ou riscos para a Administração.
 - . Promover as pertinentes penalizações e fazer os contatos necessários em nome do Tribunal.
 - . Promover os pertinentes ajustes no contrato.
 - . Conduzir o encerramento do contrato.
- 3.2.3 Fiscal do Contrato: Servidor a ser oportunamente designado mediante portaria, em obediência ao Manual de Gerenciamento e Fiscalização de Contratos do Tribunal de Justiça e ao Decreto Judiciário nº 379, de 8 de maio de 2018, com as seguintes responsabilidades:
- . Verificar os recursos materiais e humanos empregados na execução dos contratos.
 - . Verificar a forma de execução do objeto do contrato.
 - . Avaliar o cumprimento de todas as obrigações contratuais.



- . Cobrar da CONTRATADA o cumprimento do contrato.
- . Promover o registro documentado de todas as ocorrências contratuais diretamente relacionadas às obrigações assentadas no contrato.
- . Manter contato com a CONTRATADA de modo a promover todo o tipo de interlocução operacional em nome do Tribunal.
- . Comunicar ao gerente do contrato as ocorrências de cumprimento e de descumprimento contratual detectadas.

3.2.4 Preposto da CONTRATADA: Como anexo ao contrato, deverá a CONTRATADA indicar, formalmente, o seu preposto como responsável pela execução, nos termos do artigo 1561, da Lei nº 9.433/05.

- . O representante nomeado pela CONTRATADA deverá ter condições de coordenar a execução do contrato e ter poderes expressos para representá-la em todos os atos do contrato, especialmente para ajustes obrigacionais registrados em atas de reuniões, termos de recebimento ou recusa de objeto a ser entregue, notificações, ofícios, e demais atos relacionados à execução do contrato.
- . Esta designação será escrita, assinada pelo representante da CONTRATADA (outorgante) e pelo próprio preposto indicado, devendo conter, no mínimo, as disposições do “**Termo de Designação de Preposto**”, **ANEXO V** deste Termo de Referência.
- . No ato da designação, a CONTRATADA deverá apresentar todas as informações de contato do preposto escolhido (endereço, telefone, celular, WhatsApp, e-mail etc.), bem como os canais específicos para o registro de solicitações, consultas, intimações, etc.
- . Havendo necessidade de realizar reuniões de planejamento e/ou ajuste da execução dos serviços, o Gestor do Contrato poderá convocar reuniões específicas, as quais o Preposto da CONTRATADA deverá comparecer no prazo máximo de 2 (dois) dias úteis.

3.3 Dinâmica da Execução

A CONTRATADA deve entregar a Solução de Firewall de Aplicações Web (WAF) através de um cluster de appliance virtual instalados no Hypervisor(s) no Datacenter do Poder Judiciário da Bahia incluindo a implantação da solução, suporte e gerenciamento, garantia e atualização.

Para tanto, a CONTRATADA deve realizar o fornecimento, licenciamento, instalação, configuração, repasse de conhecimento, suporte técnico, garantia e atualização permanente dos itens da solução a ser entregue conforme especificações do **Tópico 4 – Requisitos Técnicos Específicos**.

A CONTRATADA deve realizar, as atividades listadas a seguir. Está definida para cada atividade a forma de atuação para a execução desta:

Atividades	Descrição sucinta da atividade	Forma de Atuação
Entrega do Appliance Virtual	Fornecimento, licenciamento e PGP. Contemplando as atividades e entregas descritas no Tópico 3.3.1 – Entrega do Appliance Virtual .	Remota, por e-mail ou senha de acesso a portal do fabricante para download
Serviço de Implantação	Instalação e configuração da solução. Contemplando as atividades e entregas descritas no Tópico 3.3.2 – Serviço de Implantação .	Presencial. Podendo ser remota sob conveniência do CONTRATANTE.
Serviço de Suporte e Gerenciamento	Atendimento de Suporte para Tratamento de Incidentes e Requisições de Serviço com 02 (duas) sessões anuais por semestre de repasse de conhecimento das configurações aplicadas na solução. Garantia e atualização permanente dos itens de software da solução. Contemplando as atividades e entregas descritas no Tópico 3.3.3 – Serviço de Suporte e Gerenciamento .	Em geral remotas. Presencial para atividades descrita no item 3.3.3.3, ou atividades que requeiram indisponibilidade do ambiente.



Atividades	Descrição sucinta da atividade	Forma de Atuação
Relatório de Operação Mensal	Conforme descrito no Tópico 3.3.4.	Remota.

Quadro 3.1 – Atividades para execução da solução de WAF

Entende-se como atividade presencial da CONTRATADA, as atividades realizadas de forma presencial na Sede do TJBA localizado no Centro Administrativo da Bahia na cidade de Salvador – BA.

A CONTRATADA deverá atender aos aspectos definidos no **Tópico 3.4 – Instrumentos Formais de Solicitação**.

A CONTRATADA deverá atender aos aspectos definidos no **Tópico 3.5 – Acordo de Níveis de Serviço**.

A implementação das políticas de segurança será de responsabilidade da CONTRATADA mediante determinações do CONTRATANTE. A implementação das políticas de segurança deverá ser realizada pela CONTRATADA em forma imediata.

O CONTRATANTE tem o direito de acessar a console administrativa da solução, com nível de administrador.

3.3.1 Entrega do Appliance Virtual

3.3.1.1 A CONTRATADA deverá realizar as seguintes entregas:

- . Entrega do Appliance Virtual conforme o Tópico 3.3.1.2.
- . Entrega da Licença conforme o Tópico 3.3.1.3.
- . PGP (Plano de Gerenciamento de Projeto) conforme o Tópico 3.3.1.4.

3.3.1.2 Entrega do Appliance Virtual – a CONTRATADA deverá entregar ao Fiscal do Contrato:

3.3.1.2.1 2(dois) appliances virtuais - conforme especificações estabelecidas no **Tópico 4 – Requisitos Técnicos Específicos**. A CONTRATADA deverá prover as máquinas virtuais que hospedarão a Solução de WAF. A CONTRATADA deverá disponibilizar todos os recursos, insumos e licenças necessárias ao pleno funcionamento da Plataforma durante toda a vigência do contrato, com as devidas atualizações de software.

3.3.1.3 Entrega do Licenciamento – a CONTRATADA deverá entregar ao Fiscal do Contrato:

- 3.3.1.3.1 As Licenças, com todas as funcionalidades habilitadas conforme especificado neste Termo de Referência.
- 3.3.1.3.2 Documentação que garanta o funcionamento do software e/ou hardware, com suporte técnico do FABRICANTE pela duração prevista de 36 meses que deve passar a ser contada a partir da emissão do TRD (Termo de Recebimento Definitivo).

3.3.1.4 PGP (Plano de Gerenciamento de Projeto)

3.3.1.4.1 PGP é um documento que deverá ser apresentado pela CONTRATADA. O CONTRATANTE deverá aprovar o PGP proposto, podendo, caso seja necessário, solicitar mais informações e/ou propor alterações visando o melhor atendimento do interesse público. Este PGP deve apresentar, no mínimo, as seguintes informações:

- . Atividades que serão executadas.
- . Produtos que serão gerados.
- . Proposta de cronograma para a execução do objeto.
- . Possíveis riscos.
- . Topologia Física e Logica a ser implementada, com detalhes de conexões física e logicas ao ambiente da Contratante.
- . Outras informações consideradas importantes para a aprovação da solicitação de serviço pelo CONTRATANTE.



- . Deverá ser realizada reunião com a Contratante para que a Contratada realize a apresentação e discussão técnica do PGP. Deve ser lavrada ata de reunião pela contratada para evidenciar a entrega técnica do PGP.

3.3.1.4.2 Após a aprovação do PGP, a CONTRATADA poderá iniciar os serviços informando, no mínimo:

- . Data de abertura.
- . Descrição dos serviços.
- . Identificação do responsável técnico da CONTRATADA.
- . Identificação do requisitante.

3.3.2 Serviço de Implantação

3.3.2.1 A CONTRATADA deverá realizar as seguintes entregas relacionada à solução WAF nas instalações físicas da sede do TJBA localizado no Centro Administrativo da Bahia na cidade de Salvador – BA, atendendo ao ANS estabelecido no Tópico **Tópico 3.5 – Acordo de Nível Serviço (ANS)**:

3.3.2.1.1 Instalação das Máquinas Virtuais no(s) Hypervisor(s) no Datacenter do Poder Judiciário da Bahia.

3.3.2.1.2 Sessão de repasse de conhecimento de no mínimo 8 horas, em 1 ou mais dias ou turnos, com a equipe técnica da contratante, visando transferir as configurações aplicadas no ambiente da contratante bem como as interligações físicas e lógicas da solução. Deve ser lavrada ata com nomes dos participantes para evidenciar a realização do repasse, com resumo dos conhecimentos transferidos

3.3.2.1.3 A contratada deverá entregar um documento de “Boas Vindas da Central de Atendimento”, orientando todos o procedimento para a abertura dos chamados, canais de contato, assim como os dados de acesso. Este documento deve estar em consonância com todos os aspectos solicitados no tópico 3.3.3 – Serviço de Suporte e Gerenciamento.

3.3.2.1.4 Implementação completa da inspeção de segurança através do web application firewall para o sistema judicial PJE com as features de segurança habilitadas, para todo tráfego de entrada do sistema seja de origem interna ou externa do TJBA.

3.3.2.1.5 Implementação completa da inspeção de segurança através do web application firewall para o sistema judicial Projudi com as features de segurança habilitadas, para todo tráfego de entrada do sistema seja de origem interna ou externa do TJBA.

3.3.2.1.6 Serão consideradas features de segurança mínimas para a entrega: a análise de SQL injection, cross-Site scripting XSS, tentativas de quebra de autenticação, análise de reputação de endereços IP públicos como fontes de ataques (DDoS, botnets, spammers, etc.), controle de acesso em massa através de robô, inspeção DDoS.

3.3.2.2 A CONTRATADA deverá prover ao CONTRATANTE informações detalhadas sobre o andamento e execução dos serviços, mantendo-as atualizadas e prontamente disponíveis, durante toda a vigência do contrato.

3.3.2.3 Ao término da etapa de implantação a CONTRATADA deverá emitir documento As-Built para aprovação do CONTRATANTE, condição para emissão do TRD (Termo de Recebimento Definitivo).

3.3.3 Serviço de Suporte e Gerenciamento

3.3.3.1 O período de garantia, suporte e licenciamento será de 36 (trinta e seis) meses, com suporte técnico de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, na Sede do TJBA localizado no Centro Administrativo da Bahia na cidade de Salvador – BA, a partir da assinatura do contrato.

3.3.3.2 Entende-se como Serviço de Suporte, toda e qualquer atividade a ser feita na solução de WAF instalada, após o Serviço de Implantação (Tópico 3.3.2), sejam requisições de serviço ou resoluções de incidentes. Abrange por exemplo, mas não somente, suporte às aplicações em produção, requisições de inclusão de novas aplicações, inclusão ou modificação dos perfis de segurança habilitados em cada aplicação e resolução de incidentes em toda a solução.



- 3.3.3.3 Dentro do Suporte à solução, o Upgrade de versões do firmware deverá necessariamente realizadas de forma presencial na Sede do TJBA localizado no Centro Administrativo da Bahia na cidade de Salvador – BA
- 3.3.3.4 A CONTRATADA deverá possuir no mínimo 1 profissional de nível superior com certificação do fabricante para a solução ofertada.
- 3.3.3.5 A CONTRATADA deverá realizar a cada 6 meses contados a partir da emissão do TRD, uma sessão de repasse de conhecimento com a CONTRATANTE de no mínimo 4 horas, visando repassar a CONTRATANTE, todas as inclusões ou alterações de configurações aplicadas no ambiente sugerindo quando necessário ajustes de melhores práticas para segurança e desempenho das aplicações configuradas no ambiente. Deve ser registrado através de ata lavrada ou chamado.
- 3.3.3.6 A CONTRATADA deverá disponibilizar ao CONTRATANTE um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada, sem ônus para o CONTRATANTE. Este serviço deverá contemplar a análise e correção de eventos relacionados à segurança e desempenho do software e do ambiente.
- 3.3.3.7 A CONTRATADA deve prover ao CONTRATANTE um Atendimento de Suporte para Requisições de Serviço e Tratamento de Incidentes. O Atendimento de Suporte, ao receber do CONTRATANTE uma solicitação, doravante denominado **chamado**, deve gerar um **Número de Chamado**. O Gestor do Contrato do PJBA definirá na Reunião de Alinhamento o profissional que poderá abrir chamados, mas poderá haver alteração deste profissional ao longo do contrato. Este Atendimento de Suporte deve possuir todas as informações que permitam a abertura dos chamados e o seu acompanhamento até o seu encerramento. O chamado só será considerado ENCERRADO quando for confirmado pelo CONTRATANTE. Este atendimento às solicitações deverá atender ao ANS estabelecido no Tópico **Tópico 3.5 – Acordo de Nível Serviço (ANS)**, onde o **Prazo de Resolução** é definido como o tempo entre a **Abertura do Chamado** e o **Encerramento deste Chamado**.
- 3.3.3.8 A CONTRATADA deve prover ao CONTRATANTE um mecanismo de Atendimento de Suporte para Tratamento de Incidentes e de Requisições de Serviço atendendo pelo menos aos seguintes aspectos:
- 3.3.3.8.1 Disponibilizar uma conta de e-mail específica para este fim.
- 3.3.3.8.2 Disponibilizar um sistema de controle dos chamados. A forma de abertura de chamados pode ser realizado pelo menos por e-mail, telefone e site. A abertura de chamado deverá ser confirmada de forma automática e instantânea pela CONTRATADA.
- 3.3.3.8.3 Ao receber uma solicitação de Tratamento de Incidente ou de Requisição de Serviço, a CONTRATADA deve responder ao e-mail do CONTRATANTE com o Número do Chamado.
- 3.3.3.8.4 Permitir a abertura de chamados, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, durante a vigência do contrato, para acesso pelo CONTRATANTE.
- 3.3.3.8.5 Arcar com todos os custos da implementação deste Atendimento de Suporte, inclusive de mão de obra (atendentes, supervisores, gerentes, etc.), equipamentos (microcomputadores dos atendentes, PABX, roteadores, etc.), mobiliários e espaço físico. A estrutura deste atendimento deve ser em ambiente externo ao CONTRATANTE e não é exigida exclusividade.
- 3.3.3.8.6 Conter, no mínimo, as seguintes informações por chamado: (a) Responsável pela abertura - CONTRATANTE, (b) Responsável pela abertura - CONTRATADA, (c) Dia/Horário de abertura, (d) Código do Chamado, (e) Causas dos defeitos, (f) Dia/Horário do Encerramento.
- 3.3.3.8.7 Permitir a solicitação eventual pelo CONTRATANTE de informação individual de chamado a ser entregue imediatamente por sistema telefônico.
- 3.3.3.9 Para chamados de Incidentes com o NSC de até 03 (três) horas, caso o atendimento não seja finalizado até as 20h00min, o técnico não poderá interrompê-lo, devendo continuar até sua finalização ou até a interrupção do mesmo pela COTEC. O chamado somente será caracterizado como “encerrado” mediante concordância da Coordenação de Suporte Técnico – COTEC.



- 3.3.3.10 Para os chamados de Requisição de Serviço, em que a solução no ambiente demande reimplantação, reestruturação ou reinstalação do produto, este deverá ser programado e planejado em conjunto com o CONTRANTE, com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas do CONTRATANTE.
- 3.3.3.11 Caso sejam necessárias ações preventivas ou corretivas, o CONTRATANTE agendará com antecedência, junto à CONTRATADA, a implementação das correções, a qual deverá ser realizada fora do horário comercial, preferencialmente em feriados e finais de semana, sem ônus para o CONTRATANTE.
- 3.3.3.12 Realizar, em tempo real, monitoramento de eventos e falhas no cluster da solução e tomar ações quando necessário. O monitoramento deverá realizar, minimamente, as seguintes verificações:
- . Checagem automática e frequente do estado do cluster;
 - . Checagem de que todos os nós do cluster estão operacionais;
 - . Checagem de que a interconexão dos nós estão funcionando corretamente;
 - . Checagem do estado de monitoramento e disparo de eventos automáticos quando necessário;
- 3.3.3.13 A CONTRATANTE deverá ser alertada pela CONTRATADA sobre todos os eventos que gerem indisponibilidade em um dos nós do cluster.
- 3.3.4 A CONTRATADA deverá entregar até o 5 (quinto) dia útil do mês posterior à prestação do serviço o **Relatório de Operação Mensal**, para aferição da qualidade de serviço, contemplando os seguintes aspectos da Etapa de Suporte:

Número do Chamado
Código do Chamado
NSC aplicável
Data/Hora Abertura
Data/Hora Encerramento
Problema
Local
Nível em que foi solucionado
Grupo Solucionador
Origem da abertura (site, telefone, whts app, etc..)
Solução aplicada

Quadro 3.2 – Layout do Relatório de Operação Mensal da Etapa Suporte

3.4 Instrumentos Formais de Solicitação

3.4.1 Reunião de Alinhamento

A reunião de alinhamento entre o CONTRATANTE e a CONTRATADA será realizada com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no contrato, edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

A reunião realizar-se-á no endereço do CONTRATANTE ou remotamente em até 5 (cinco) dias úteis após a publicação do contrato. Será remota, por conveniência do CONTRATANTE ou caso as condições relativas à saúde pública não permitam, ou autorizem, reuniões presenciais. A reunião ocorrerá conforme agendamento efetuado pelo CONTRATANTE, através do Gestor do Contrato

Nessa reunião a CONTRATADA deverá:

- . Apresentar oficialmente seu INTERLOCUTOR (Preposto ou Gerente de Contrato), designando-o mediante **Termo de Designação de Preposto**, cujo modelo segue no **ANEXO V**.
- . Apresentar um Planejamento global da execução passando pelos aspectos estabelecidos no **Tópico 3.3 – Dinâmica da Execução**. Deve-se apresentar cronograma de atendimento em conformidade com o **Tópico 3.5 – Acordo de Nível Serviço (ANS)**, contemplando os serviços oferecidos e quais



tecnologias serão utilizadas na solução, de maneira a demonstrar o atendimento a todos os requisitos exigidos neste Termo de Referência. Todos estes aspectos deverão ser aprovados pelo CONTRATANTE.

3.4.2 Requisições de Serviço e Tratamento de Incidentes

Estes serviços a serem prestados são de natureza técnica, sob demanda, e serão solicitados pelo CONTRATANTE por meio de Chamado, conforme detalhado no **Tópico 3.3.3 – Serviço de Suporte e Gerenciamento**.

3.5 Acordo de Nível de Serviços

Considerando que o preço ajustado em contrato se refere à execução com a máxima qualidade, o valor total a ser pago pela realização dos serviços, objeto deste termo de referência, será proporcional à qualidade da entrega dos serviços, o que será apreciado mediante identificação e quantificação de ocorrências e tabelamento de respectivo efeito remuneratório percentual. Tais ajustes asseguram ao Poder Judiciário no Estado da Bahia e à CONTRATADA o recebimento dos serviços mesmo diante de eventuais ocorrências de menor qualidade em sua execução, com a dedução prevista no artigo 164 da Lei Estadual nº 9.433/05 pela fração quantitativa ou qualitativa objetivamente verificada pelo preenchimento do **Relatório de Operação Mensal** nos termos do tópico 3.3.4.

Considera-se que o serviço foi atendido pela CONTRATADA da forma estabelecida neste Termo de Referência, se a ação/atividade prevista, tenha sido realizada dentro do **Nível de Serviço Contratado (NSC)**, estabelecido para as diversas ações/atividades a serem executadas pela CONTRATADA.

O atendimento proporcional do serviço pela CONTRATADA da forma estabelecida neste Termo de Referência, gerará o indicador **Entrega Proporcional (EP)** que expressa, em relação ao total mensal, a percepção do CONTRATANTE da entrega em relação à quantidade e/ou qualidade contratadas. Este **EP** será utilizado no cálculo do pagamento da fatura conforme expresso no **Tópico 3.8 – Forma de Pagamento**.

3.5.1 Cálculo do indicador **EP** (Entrega Proporcional) para o **Serviço de Implantação** nos termos estabelecidos no **Tópico 3.3.2**.

Os quadros a seguir apresentam os aspectos associados ao cálculo e aplicação.

Atividade	Nível de Serviço Contratado (NSC)
Implantação.	Em até 30 (trinta) dias corridos a partir da Emissão do TRP (Termo de Recebimento Provisório).

Quadro 3.3 – Nível de Serviço Contratado para Serviço de Implantação

NSC	EP
ATENDIDO	1
INFRINGIDO até 5 dias corridos	0,8
INFRINGIDO até 10 dias corridos	0,6
INFRINGIDO a partir 10 dias corridos	0,4

Quadro 3.4 – Cálculo do EP para Serviço de Implantação

Atividade	Aplicação do EP
Implantação	Fatura associada ao pagamento do Item 3 da Proposta Comercial.

Quadro 3.5 – Fatura em que deverá ser aplicado o EP da Etapa de Implantação.

3.5.2 Cálculo do indicador **EP** (Entrega Proporcional) para o **Serviço de Suporte e Gerenciamento** nos termos estabelecidos no **Tópico 3.3.3**.



Os quadros a seguir apresentam os aspectos associados ao cálculo e aplicação.

Código	Chamados	Nível de Serviço Contratado (NSC)
CH-1	Resolução de solução totalmente indisponível	Até 3 horas
CH-2	Resolução de um dos appliances virtuais (alta disponibilidade) indisponível.	Até 72 horas
CH-3	Resolução de serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso das aplicações – Sistemas Judiciais.	Até 6 horas
CH-4	Resolução de serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso das aplicações – Sistemas Não Judiciais.	Até 72 horas
CH-5	Atendimento a aplicações (Sistemas Judiciais) em produção no Web Application Firewall.	Até 8 horas
CH-6	Atendimento a aplicações (Sistemas Não Judiciais) em produção no Web Application Firewall.	Até 48 horas
CH-7	Atendimento a aplicações que não estejam em produção no Web Application Firewall e demais requisições.	Até 72 horas

Quadro 3.6 – Nível de Serviço Contratado por Chamado por Serviço de Suporte

			Fator de Significância		
			NSC	NSC	NSC
Horas Infringidas			Até 3 hrs	Até 6 hrs	Até 8 hrs
0	à	1	2	1	1
1	à	2	3	2	1
2	à	3	5	3	1
3	à	4	7	4	1
4	à	6	9	5	2
6	à	8	11	6	2
8	à	12	13	7	2
12	ou	>	15	8	2

			Fator de Significância	
			NSC	NSC
Horas Infringidas			Até 48 hrs	Até 72 hrs
0	à	4	1	1
4	à	8	1	1
8	à	16	1	1
16	à	24	1	1
24	à	48	1	1
48	à	72	1	1
72	à	96	1	1
96	ou	>	1	1

Quadro 3.7 – Tabela de Significância por Horas Infringidas

Somatório das **Horas Infringidas Significativas** por Chamados Encerrados no mês

$$EP = 1 - \frac{\text{Somatório das Horas Infringidas Significativas}}{\text{Total de Horas da Prestação do Serviço no mês} = (24 \times \text{num de dias corridos do mês})}$$

Variáveis:

Hora Infringida – quantidade de horas que a CONTRATADA levou para atender ao chamado que ultrapassaram o NSC estabelecido. A fração de hora será desconsiderada. Por exemplo: 3,2 horas será considerado 3 horas, 4,7 horas será considerado 4 horas.

Hora Infringida Significativa – Por exemplo, seja um chamado com número de *Horas Infringidas* de 3 (três) horas no NSC Até 3 hrs. Para o cálculo das *Horas Infringidas Significativas*, relacionado a estas *Horas Infringidas*, inicialmente distribui-se a *Hora Infringida* do Chamado pelas respectivas faixas associadas. Neste caso esta quantidade de *Horas Infringidas* utilizará as três primeiras faixas da coluna:

- 1ª Faixa – 0 à 1 - Fator de Significância = 2 * 1h (*Hora Infringida*) = 2h (*Horas Infringidas Significativas*)
- 2ª Faixa – 1 à 2 - Fator de Significância = 3 * 1h (*Hora Infringida*) = 3h (*Horas Infringidas Significativas*)
- 3ª Faixa – 2 à 3 - Fator de Significância = 5 * 1h (*Hora Infringida*) = 5h (*Horas Infringidas Significativas*)

Desta forma, neste exemplo, para 3 (três) *Horas Infringidas*, teremos 10 (dez) *Horas Infringidas Significativas*

Quadro 3.8 – Cálculo do EP para a Etapa de Suporte

Atividade	Aplicação do EP
Suporte	Faturas associadas ao pagamento mensal do Item 4 da Proposta Comercial.

Quadro 3.9 – Fatura em que deverá ser aplicado o EP da Etapa de Suporte.



3.6 Acompanhamento da Execução

O Preposto, indicado pela CONTRATADA como seu representante na reunião de alinhamento, será o responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual. Este serviço, de gerenciamento do contrato e dos diversos serviços nele contemplados, será prestado sem ônus específico.

Da parte do CONTRATANTE, o gestor e o fiscal do contrato, através de ferramentas próprias, serão encarregados do monitoramento dos serviços contratados.

Como meios de comunicação oficiais entre o CONTRATANTE e a CONTRATADA, poderão ser utilizados os seguintes: E-mail, Relatório de Operação Mensal, Termo de Notificação e Relatórios gerados pelo Sistema de Informação utilizado na prestação dos serviços.

3.7 Recebimento Provisório e Definitivo

O PJBA designará servidor responsável para realizar o recebimento dos objetos, da seguinte forma:

3.7.1 Termo de Recebimento Provisório

O Termo de Recebimento Provisório será emitido pelo CONTRATANTE quando a CONTRATADA realizar a Entrega do Appliance Virtual nos termos estabelecidos no **Tópico 3.3.1**.

3.7.3 Termo de Recebimento Definitivo

Será emitido ao final da etapa de implantação, um termo de Recebimento Definitivo para os itens 1,2 e 3, uma única vez, o que é condição de habilitação para o pagamento dos itens 1,2 e 3. O TRD será anexado mensalmente ao processo de pagamento.

Ao final dos 36 meses, será emitido um TRD para o item 4 – Suporte e Gerenciamento, confirmando que os serviços foram prestados adequadamente. Para os pagamentos mensais a CONTRATANTE irá gerar o **Relatório de Serviços e Qualidade Percebida**, conforme descrito no **Tópico 3.8 - Forma de Pagamento**.

O Termo de Recebimento Definitivo da totalidade dos serviços, nos termos do Art 161 da Lei 9433/2005, habilitando a CONTRATADA a requerer a devolução da caução, será emitido após o encerramento do contrato mediante constatação de que todas as obrigações da CONTRATADA foram satisfatoriamente executadas, inclusive todos os aspectos do **Tópico 3.9 – Transferência de Conhecimento**.

3.8 Forma de Pagamento

O pagamento observará o roteiro apresentado no edital e será efetuado, conforme modelo de proposta do **ANEXO II – Modelo de Proposta Comercial**. O desembolso ocorrerá conforme a seguinte sequência:

ID	Evento	Quando	Prazo em dias até	Quem
1	Assinatura do Contrato	Início	Não se aplica	Ambos
2	Reunião de Alinhamento	Após Publicação do Contrato	5 dias úteis	Ambos
3	Entrega do Appliance Virtual nos termos do Tópico 3.3.1 associado aos valores dos Itens 1 e 2 da Proposta Comercial.	Após Publicação do Contrato	30 dias corridos	Contratada
4	Emissão do TRP (Termo de Recebimento Provisório)	Após ID 3	5 dias corridos	Contratante
5	Serviço de Implantação nos termos do Tópico 3.3.2 associado ao valor do Item 3 da Proposta Comercial.	Após Emissão do TRP	30 dias corridos	Contratada
6	Emissão do TRD (Termo de Recebimento Definitivo) para os Itens 1, 2 e 3 da Proposta Comercial.	Após ID 5	7 dias corridos	Contratante
7	Pagamento dos Itens 1 e 3 da Proposta Comercial	Após ID 6	8 dias úteis	Contratante



ID	Evento	Quando	Prazo em dias até	Quem
8	Início da atividade de Serviço de Suporte e Gerenciamento nos termos do Tópico 3.3.3 associado ao valor mensal do Item 4 da Proposta Comercial	Após entrega do ID 6	Imediato	Contratada
9	Emissão do Relatório de Operação Mensal	Todo o mês após ID 5	5º dia útil do mês subsequente à prestação dos serviços	Contratada
10	Emissão do Instrumento de Medição de Resultado (IMR)	Todo o mês após ID 5	10 dias úteis	Contratante
11	Pagamento mensal dos itens 2 e 4. Licenciamento e serviços de suporte contidos no Instrumento de Medição de Resultado (IMR).	Todo mês após ID 6	8 dias úteis	Contratante

Quadro 3.10 – Cronograma de desembolso

Os pagamentos começarão a partir do evento de liberação de pagamento conforme **Quadro – Cronograma de desembolso associados aos eventos**, com fatura a ser emitida no final do mês em que este evento ocorra, para ser pago pelo CONTRATANTE a partir do mês subsequente.

Em atenção aos princípios da economicidade e da eficiência, a remuneração dos **Serviços** estará vinculada ao atendimento de Níveis de Serviço. Para o acompanhamento e avaliação dos serviços efetuados pela CONTRATADA será estabelecido e utilizado o Acordo de Nível de Serviço (doravante ANS) entre as partes conforme o **Tópico 3.5 – Acordo de Níveis de Serviço**. O ANS deve ser considerado e entendido pela CONTRATADA como um compromisso do padrão de serviço que estará assumindo junto ao CONTRATANTE.

O valor a ser pago pela realização dos serviços será apurado em razão do cumprimento do Acordo de Nível de Serviço (ANS) podendo, diante do não atendimento, resultar em glosa no seu pagamento. Entretanto, eventuais falhas e descumprimentos contratuais verificados serão devidamente apurados em processos administrativos próprios, podendo resultar em aplicação de penalidade, sem prejuízo de possível rescisão do contrato, na forma prevista na lei.

Para este contrato a tabela a seguir associa os serviços a serem pagos de forma proporcional com os Itens da Proposta Comercial, conforme ANS definido no Tópico 3.5.

Etapa	Item da Proposta Comercial
Serviço de Implantação nos termos do Tópico 3.3.2	Item 3
Serviço de Suporte e Gerenciamento nos termos do Tópico 3.3.3	Item 4

Consoante a esta abordagem, para o estabelecimento da remuneração mensal da CONTRATADA em relação aos serviços prestados, define-se:

- . Pagamento Completo (PC) [R\$]: valor de referência acordado com a CONTRATADA para o pagamento do serviço. O PC a ser considerado é o **valor** do Item/Subitem estabelecido na Proposta Comercial final entregue pela empresa vencedora do certame.
- . Entrega Proporcional (EP): indicador de proporcionalidade do serviço realizado pela CONTRATADA calculado a partir das regras estabelecidas no **Tópico 3.5 – Acordo de Níveis de Serviço**.
- . Valor da Fatura (VF) [R\$]: valor efetivo a ser pago à CONTRATADA pelo CONTRATANTE referente ao pagamento completo (PC) proporcional à entrega.

$$VF = PC * EP$$

Caso o **EP apurado** no mês seja igual ou inferior a 0,7, o **EP utilizado** será limitado a 0,7 e o cálculo do VF é expresso pela seguinte fórmula:

$$VF = PC * 0,7$$



Se, ao longo de um período de 6 (seis) meses consecutivos, o **EP apurado** do serviço entregue pela CONTRATADA for inferior a 0,7 por 03 (três) meses consecutivos ou não, o CONTRATANTE poderá aplicar as sanções previstas na Lei de Licitações 8.666/93.

Para todos os fins, será considerado o mês de atividade referente ao serviço realizado a partir de 0:00h do 1º dia até as 23:59h do último dia do mês. A efetivação e aceite de quaisquer serviços não previstos só poderá acontecer mediante aprovação formal do CONTRATANTE.

O Valor da Fatura (VF) deverá ser atestado pelo Gestor e Fiscal do Contrato, estando condicionado à apuração das atividades através do ANS estabelecido no Tópico 3.5 – Acordo de Níveis de Serviço. Para esta apuração, até o 5º (quinto) dia útil de cada mês, A CONTRATADA deverá encaminhar o **Relatório de Operação Mensal** conforme especificação no **Tópico 3.5.3**.

O CONTRATANTE avaliará o **Relatório de Operação Mensal** em até 10 (dez) dias úteis, encaminhando para a CONTRATADA o **Instrumento de Medição do Resultado** com o Valor da Fatura já com as glosas referente ao ANS. Após a CONTRATADA encaminhar a Fatura e demais documentos necessários para o pagamento, o CONTRATANTE terá até 8 (oito) dias úteis para efetuar o pagamento. Para este CONTRATO será utilizado o seguinte modelo para geração do **Instrumento de Medição do Resultado**:

Instrumento de Medição de Resultado					Mês: MM/AAAA		
Item / SubItem	Descrição	Valor Unitário (R\$)	Qtde	PC (R\$)	EP apurado	EP utilizado	Valor da Fatura (R\$)
1	Virtual Appliance					1	
2	Licenciamento da solução, suporte e atualizações do fabricante por 36 meses					1	
3	Serviço de Implantação						
4	Serviço de Suporte						
Valor da Fatura – Total – R\$							

Quadro 3.11 – Layout do Instrumento de Medição de Resultado

3.9 Transferência de Conhecimento

A CONTRATADA deverá efetuar o registro de todo o processo de migração, bem como de todos os atendimentos de garantia, suporte e atualização, e disponibilizar esses registros ao CONTRATANTE sempre que solicitado.

Será franqueado aos técnicos do CONTRATANTE o acompanhamento de todas as intervenções realizadas, bem como serão prestadas todas as informações que os mesmos solicitem para melhor compreensão das ações e respectivos resultados

Em caso de mudança de fornecedor, o CONTRATANTE realizará uma reunião de alinhamento de expectativas com NOVA CONTRATADA para dar início formal à transferência de conhecimentos entre as empresas.

Os meios utilizados para essa transferência serão previamente acordados entre CONTRATADA e CONTRATANTE, podendo consistir em um ou uma combinação dos seguintes meios:

- Divulgação eletrônica.
- Base de conhecimentos.
- Registro de lições aprendidas.
- Registro de soluções alternativas utilizadas.
- Registro de ocorrências, conhecimentos e procedimentos.
- Documentação de melhores práticas.
- Reuniões e suas respectivas atas.
- Relatórios periódicos.
- Ferramentas de comunicação em geral (videoconferência, chat, e-mail etc.).



3.9.1 Transição Contratual

A CONTRATADA deverá, em conformidade com o parágrafo único do artigo 111 da Lei nº 8.666/93, promover transição contratual e repassar para o CONTRATANTE e/ou para a nova CONTRATADA todos os dados, documentos e elementos de informação utilizados na execução dos serviços.

Caso o LICITANTE vencedor não seja a atual CONTRATADA do PJBa para a prestação dos serviços, a NOVA CONTRATADA deverá apresentar um plano de migração do serviço existente.

Em data prevista no plano de migração, a NOVA CONTRATADA deverá acionar o CONTRATANTE com vistas a agendar atendimento conjunto com a CONTRATADA.

As atividades de migração poderão ocorrer de forma paralela ou sequencial, desde que não seja ultrapassado o prazo final estipulado com o CONTRATANTE.

3.9.2 Encerramento Abrupto do Contrato

Em caso de encerramento abrupto do contrato, será necessário um novo contrato para o atendimento dos serviços entregues. A operação do sistema não será afetada diretamente e os serviços não sofrerão descontinuidade. Portanto, competirá ao PJBA:

. Iniciar imediato planejamento de nova contratação para substituir a contratação.

3.10 Direitos de Propriedade Intelectual

A contratação não envolverá geração de produtos que possam ser objeto de registro de propriedade intelectual.

3.11 Qualificação Técnica Profissional

A composição da equipe técnica que prestará os serviços deverá ser provida e dimensionada pela CONTRATADA, estabelecendo adequada relação entre as obrigações assumidas e a quantidade, qualificação e produtividade individual dos profissionais que deverão executá-las. Cabendo ao CONTRATANTE exigir a prestação adequada e aderente às condições exigidas.

A CONTRATADA deverá possuir no mínimo 1 profissional de nível superior com certificação do fabricante para a solução ofertada.

3.12 Garantia Contratual

Em garantia de plena, fiel e segura execução de tudo o que se há obrigado, a CONTRATADA prestará caução correspondente a 5% (cinco por cento) sobre o valor global do objeto contratado, em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, cuja liberação ou restituição dar-se-á após a expiração deste instrumento contratual.

A garantia será obrigatoriamente revista e complementada quando houver redução da sua representatividade percentual por variação econômica do contrato ou descontos de valores devidos ao CONTRATANTE, a exemplo de multas, quando for o caso.

A garantia responderá pelo inadimplemento das obrigações contratuais e pelas multas impostas, independentemente de outras cominações legais.

O cálculo da atualização monetária do valor caucionado em dinheiro será feito aplicando-se o índice mais vantajoso para a Administração entre a data de retenção da caução e da devolução do seu valor.

A garantia deverá ser apresentada no prazo máximo de 10 (dez) dias corridos, contados da assinatura do Contrato.

3.13 Descumprimento das Obrigações Contratuais

Com fundamento nos artigos constantes da Seção VII do Capítulo IX da Lei Estadual nº 9.433/2005 e nos artigos constantes do Capítulo XI da Lei Estadual nº 9.433/2005, nas normas das Leis Federais nº 8666/1993 e nº 10520/2002, bem como nos decretos Judiciário nº 12/2003 e nº 44/2003, a CONTRATADA ficará sujeita às sanções previstas em contrato no caso de descumprimento das obrigações pactuadas, sem prejuízo das responsabilidades civil e criminal, e assegurada a prévia e ampla defesa.



TJBA – Tribunal de Justiça do Estado da Bahia

SETIM / DMO / CPROM

À CONTRATADA que incorrer nas faltas administrativas previstas na Legislação serão aplicadas, sem prejuízo do disposto no art. 186, parágrafo único da Lei Estadual nº 9.433/2005, as penalidades de acordo com o art. 192 da Lei Estadual nº 9.433/2005.

As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

As multas não impedem que a Administração rescinda unilateralmente o contrato e aplique as demais sanções previstas na lei, bem como não têm caráter compensatório e o seu pagamento não eximirá a CONTRATADA da responsabilidade por perdas e danos decorrentes das infrações cometidas.

Para a aplicação das penalidades previstas, será levada em conta a natureza e a gravidade da falta, os prejuízos dela advindos para a Administração Pública e a reincidência na prática do ato.

Nesse caso, o CONTRATANTE aplicará as sanções previstas na Lei de Licitações nº 9.433/05.

Outras sanções poderão eventualmente ser impostas à CONTRATADA de acordo com a legislação aplicável.



4 Requisitos Técnicos Específicos

Lista inicial dos sistemas que são candidatos a implementação pela solução

<https://pje.tjba.jus.br/pje-web/>
<http://esaj.tjba.jus.br/esaj/portal.do?servico=740000>
<https://projudi.tjba.jus.br/projudi/>
<https://saipro.tj.ba.gov.br>
www.tjba.jus.br
<https://www9.tjba.jus.br/gefre>
<https://www2.tjba.jus.br/rhnet2/>
<https://www9.tjba.jus.br/srh2>
<https://www2.tjba.jus.br/portaldrh/home>
<http://www2.tjba.jus.br/rhnet>
<https://www9.tjba.jus.br/precatorio>
<http://www3.tjba.jus.br:8081/wipass/index.wsp>
<http://www7.tjba.jus.br/ar/index.wsp>
<https://eselo.tjba.jus.br/>
<http://www2.tjba.jus.br/scr>
<https://www.tjba.jus.br/ouvidoria/#/>
<http://alvaraeletronico.tjba.jus.br:80/alvarabb>
<http://sigaapp001:8080/siga/principal.action>
<https://www9.tjba.jus.br/precatorio>
<https://migracaopje.tjba.jus.br/migracaoaipro/home#!/login>

4.1 Requisitos Mínimos de Performance

- 4.1.1 Introduzir baixa latência, a fim de não impactar a performance das aplicações Web;
- 4.1.2 Deve possuir throughput mínimo para HTTP de 2.4 Gbps;
- 4.1.3 Deve suportar instalação em sistemas com processadores em 64-bits;
- 4.1.4 Deve suportar até 64GB de memória em sistemas processado em 64-bits;
- 4.1.5 Deve suportar no mínimo, 8vCPU para cada appliance virtual
- 4.1.6 Possuir área de armazenamento interno de no mínimo 2 GB.

4.2 Requisitos Mínimos de Funcionalidade

- 4.2.1 A solução deve ser fornecida em Alta Disponibilidade (HA).
- 4.2.2 O equipamento deve ser baseado em appliance virtual a ser implementada em Hypervisor(s) pré-existente e deve possuir softwares específicos, destinados à finalidade de Firewall de Aplicação Web (WAF), bem como as licenças necessárias, conforme requerido neste termo de referência, para o seu funcionamento e proteção de servidores e aplicações Web.
- 4.2.3 A solução deve suportar, através da compatibilidade de instalação, os seguintes fabricantes/desenvolvedores/hypervisors: VMWare, Microsoft (Hyper-V) e KVM.
- 4.2.4 A solução deve suportar, através da compatibilidade de instalação e licenciamento transparente (Bring Your Own Licence, ou BYOL), a migração e consequente instalação da solução completa em ambiente/hypervisor de nuvem pública, com todas as funcionalidades definidas nesse documento, especificamente para os seguintes provedores de nuvem pública: Amazon (AWS), Microsoft (Azure) e Google (GCP)



4.3 Funcionalidades de Rede

- 4.3.1 A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso), Passivo, ou “Sniffer” (Offline) e Inline Transparente (Bridge).
- 4.3.2 A solução deve ser capaz de ser implementada com protocolo WCCP.
- 4.3.3 Suportar VLANs no padrão IEEE 802.1q.
- 4.3.4 Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP) - IEEE 802.3ad.
- 4.3.5 Suportar endereçamento IPv4 e IPv6 nas interfaces (inclusive VLANs).
- 4.3.6 A solução ofertada deve oferecer cluster de alta disponibilidade entre dois dispositivos no modo Ativo-Passivo e Ativo-Ativo, para que quando o principal falhar o tráfego possa continuar sendo processado.
- 4.3.7 A solução deve suportar a sincronização de configuração entre dois appliances iguais, com o objetivo de operar no modo ativo-ativo, com a distribuição de tráfego sendo realizada por balanceador de carga externo ou pela própria solução.
- 4.3.8 A solução deve suportar roteamento por política (policy route).

4.4 Funcionalidades de Gerência

- 4.4.1 O sistema operacional / firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, e através de CLI (interface de linha de comando), acessando localmente, via porta de console, ou remotamente via SSH.
- 4.4.2 Deve possuir administração baseada em interface web HTTPS.
- 4.4.3 Possuir auto-complementação de comandos na CLI.
- 4.4.4 Possuir ajuda contextual na CLI.
- 4.4.5 A solução deve possuir Interface Gráfica com informações sobre o sistema Ex: (Informações do Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware).
- 4.4.6 Deverá ser possível visualizar através da interface gráfica de gerência informações de licenças e assinaturas.
- 4.4.7 Deve prover, na interface de gerência, as seguintes informações do sistema para cada gateway: consumo de CPU e estatísticas das conexões.
- 4.4.8 Deve ser possível visualizar na interface de gerência as informações de consumo de memória.
- 4.4.9 Deve ser possível visualizar na interface de gerência ou CLI as informações de utilização de disco de log.
- 4.4.10 Deverá possuir ferramenta, na interface gráfica de gerência (dashboard) que permita visualizar os últimos logs de ataque detectados/bloqueados.
- 4.4.11 Deve prover as seguintes informações, na interface de gráfica de gerência: estatísticas de throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema.
- 4.4.12 Possuir na interface gráfica estatísticas de conexões concorrentes e por segundo, de políticas de segurança do sistema.
- 4.4.13 Possuir um painel de visualização com informações das interfaces de rede do sistema.
- 4.4.14 A configuração de administração da solução deve possibilitar a utilização de perfis.
- 4.4.15 Deve ser possível executar e restaurar backup via interface Web (GUI).
- 4.4.16 Deve ter a opção para criptografar o backup.



- 4.4.17 Deve ser possível executar e restaurar backup utilizando-se um ou mais dos seguintes protocolos: FTP, SFTP e/ou TFTP"
- 4.4.18 Deve ser possível instalar um firmware alternativo em disco e inicializá-lo em caso de falha do firmware principal.
- 4.4.19 Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3.
- 4.4.20 Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog.
- 4.4.21 A solução deverá ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG.
- 4.4.22 Ter a capacidade de armazenar logs em appliance remoto.
- 4.4.23 A solução deve ter a capacidade de adicionar identificadores customizados nos registros syslog antes de envio, como hostname, atrelados a valores fixos ou variáveis.
- 4.4.24 A solução deve ter a capacidade de enviar alertas por e-mail de eventos baseados em severidades e/ou categorias.
- 4.4.25 A solução deve possuir dados analíticos contendo localização geográfica dos clientes web.
- 4.4.26 A solução deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem , o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (hits) e percentual de cada país de origem.
- 4.4.27 Deverá ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário.
- 4.4.28 Deve ter suporte a RESTful API para gerenciamento de configurações.
- 4.4.29 Deve suportar todas as funcionalidades para comunicação HTTP/2

4.5 Funcionalidades de Autenticação

- 4.5.1 Os usuários devem ser capazes de autenticar através do cabeçalho de autorização HTTP / HTTPS.
- 4.5.2 Os usuários devem ser capazes de autenticar através de formulários HTML embutidos.
- 4.5.3 A solução deverá ser capaz de autenticar usuários através de certificados digitais pessoais.
- 4.5.4 Deve possuir base local para armazenamento e autenticação contas de usuários.
- 4.5.5 A solução deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS.
- 4.5.6 Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM.
- 4.5.7 A solução deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação.

4.6 Funcionalidades de Web Application Firewall

- 4.6.1 Deverá ser capaz de identificar e bloquear ataques através de reputação de Endereços IPs atualizado de forma automática.
- 4.6.2 Deverá ser capaz de identificar e bloquear ataques através um banco de dados de assinaturas de vírus ou integrar com servidor ICAP, atualizado de forma automática.
- 4.6.3 Deverá implementar recurso de machine learning, onde será permitido implementar proteção para um servidor ou grupo de servidores de aplicação web, de forma automatizada através da análise da utilização da aplicação, fazendo a descoberta da estrutura e padrões e padrões de uso, buscando separar o comportamento anormal do abusivo, detectando anomalias e tentativas de ataque.
- 4.6.4 Ter a capacidade de criação de assinaturas de ataque customizáveis.



- 4.6.5 Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol.
- 4.6.6 Ter a capacidade de proteção para ataques do tipo Botnet.
- 4.6.7 Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST).
- 4.6.8 A solução deverá possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta.
- 4.6.9 Deve suportar detecção a ataques de Clickjacking.
- 4.6.10 Deve suportar detecção a ataques de alteração de cookie.
- 4.6.11 Identificar e prevenir ataques do tipo Credit Card Theft.
- 4.6.12 Identificar e prevenir ataque Cross Site Request Forgery (CSRF).
- 4.6.13 A solução deverá possuir funcionalidade de proteção positiva contra ataques como cross site scripting (XSS).
- 4.6.14 Deve possuir proteção contra ataques de Denial of Service (DoS).
- 4.6.15 Ter a capacidade de proteção para ataques do tipo HTTP header overflow.
- 4.6.16 Ter a capacidade de proteção para ataques do tipo Local File inclusion (FLI).
- 4.6.17 Ter a capacidade de proteção para ataques do tipo Man-in-the-middle (MITM).
- 4.6.18 Ter a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI).
- 4.6.19 Ter a capacidade de proteção para ataques do tipo Server Information Leakage.
- 4.6.20 Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection).
- 4.6.21 Ter a capacidade de proteção para ataques do tipo Malformed XML.
- 4.6.22 Identificar e prevenir ataques do tipo Low-rate DoS.
- 4.6.23 Prevenção contra Slow POST attack.
- 4.6.24 Proteger contra ataques Slowloris.
- 4.6.25 Ter a capacidade de proteção para ataques do tipo SYN flood.
- 4.6.26 Ter a capacidade de proteção para ataques do tipo Forms Tampering.
- 4.6.27 A solução deverá possuir funcionalidade de proteção positiva contra ataques de manipulação de campo escondido.
- 4.6.28 Ter a capacidade de proteção para ataques do tipo Directory Traversal.
- 4.6.29 Ter a capacidade de proteção do tipo Access Rate Control.
- 4.6.30 Ter a habilidade de configurar proteção do tipo TCP SYN flood-style para prevenção de DoS para qualquer política, através de Syn Cookie e Half Open Threshold.
- 4.6.31 Permitir configurar regras de bloqueio a métodos HTTP indesejados.
- 4.6.32 Permitir que sejam configuradas regras de limite de upload por tamanho de arquivo.
- 4.6.33 Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país.
- 4.6.34 Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado país seja bloqueado.
- 4.6.35 Permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem.



- 4.6.36 Permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.
- 4.6.37 Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation.
- 4.6.38 Ter a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP.
- 4.6.39 Ter a funcionalidade de proteger o website contra ações de desfiguração (defacement), ou implementar proteções para impedir exploração de vulnerabilidades que resultem em ações de desfiguração (defacement).
- 4.6.40 Ter a funcionalidade de antivírus ou integração para inspeção de tráfego e arquivos via servidor ICAP.
- 4.6.41 Ter a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não-conformidade.
- 4.6.42 Deverá ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia.
- 4.6.43 A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego.
- 4.6.44 Para SSL/TLS offload suportar no mínimo TLS 1.0, 1.1, 1.2 e 1.3.
- 4.6.45 A solução deve ter a capacidade de armazenar certificados digitais de CA's.
- 4.6.46 A solução deve ser capaz de gerar CSR para ser assinado por uma CA.
- 4.6.47 A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL).
- 4.6.48 A solução deve conter as assinaturas de robôs conhecidos como link checkers, indexadores de web, search engines, spiders e web crawlers que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões.
- 4.6.49 A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers, etc. Tal sistema deve ser atualizado automaticamente.
- 4.6.50 A solução deverá ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores.
- 4.6.51 A solução deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location.
- 4.6.52 A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessados para prevenir ataques como cross-site request forgery (CSRF).
- 4.6.53 A solução deve ter a capacidade de definir restrições a métodos HTTP.
- 4.6.54 A solução deve ter a capacidade de proteger contra a detecção de campos ocultos.
- 4.6.55 Permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares.
- 4.6.56 A solução deve incluir capacidade de atuar como um scanner de vulnerabilidades ou permitir a integração com scanners de vulnerabilidade de terceiros que realizem diagnóstico e identificação de ameaças nos servidores web, software desatualizado e potenciais buffers overflows,
- 4.6.57 Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros.
- 4.6.58 A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML, ou um relatório das políticas implementadas a partir da importação de um arquivo em formato XML da análise de terceiros.



- 4.6.59 A solução deve permitir a exclusão de URLs na análise de vulnerabilidades, ou permitir a exclusão de URLs na implementação das políticas de mitigação geradas a partir da análise de terceiros.
- 4.6.60 Deverá ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente.
- 4.6.61 Suportar redireção e reescrita de requisições e respostas HTTP.
- 4.6.62 Permitir redirecionar requisições HTTP para HTTPS.
- 4.6.63 Permitir reescrever a linha URL no cabeçalho de uma requisição HTTP.
- 4.6.64 Permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP.
- 4.6.65 Permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP.
- 4.6.66 Permitir redirecionar requisições para outro web site.
- 4.6.67 Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP.
- 4.6.68 Permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web.
- 4.6.69 Permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor web.
- 4.6.70 Permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso.
- 4.6.71 A solução deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (rate limit).
- 4.6.72 A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizando mecanismos como HTML Form, Basic e Suporte a SSO, métodos como LDAP e RADIUS para consultas e integração dos usuários da aplicação.
- 4.6.73 Possuir capacidade de caching para aceleração web.
- 4.6.74 Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.
- 4.6.75 Deve suportar no mínimo 500 regras de reescrita URL distintas
- 4.6.76 Deve suportar no mínimo 250 políticas de assinatura distintas
- 4.6.77 Deve suportar no mínimo 500 grupos ou pools de servidores, e cada pool deve suportar no mínimo 1000 membros
- 4.6.78 Deve suportar no mínimo 1000 IPs virtuais configurados e ativos simultaneamente
- 4.6.79 Deve ser capaz de restringir acesso quando as requisições não tiverem um cabeçalho HTTP específico pré-configurado
- 4.6.80 Deve ser capaz de limitar o número de usuários/origens simultâneos acessando a mesma conta/sessão/login.
- 4.6.81 Deve ser capaz de criptografar URLs.
- 4.6.82 Deve ser capaz de adicionar múltiplos servidores ADFS em um pool de servidores

4.7 Funcionalidades de Balanceamento de Carga

- 4.7.1 A solução deve incluir funcionalidade de balanceamento de carga entre servidores web.
- 4.7.2 Deve ter a habilidade de configurar portas não-padrão para aplicação web HTTP e HTTPS.
- 4.7.3 Ter a capacidade de balancear/distribuir tráfego e rotear o conteúdo através de vários servidores web.



- 4.7.4 A solução deve permitir criar grupos de servidores (Server Farm / Pool) para distribuir as conexões dos usuários.
- 4.7.5 Suportar algoritmo Round Robin para balanceamento de carga de servidores.
- 4.7.6 Suportar algoritmo Weighted Round Robin para balanceamento de carga de servidores.
- 4.7.7 Suportar algoritmo Least Connections para balanceamento de carga de servidores.
- 4.7.8 A solução deve ser capaz de criar servidores virtuais que definem a interface de rede/bridge e endereço IP por onde o tráfego destinado ao Server Pool é recebido.
- 4.7.9 Os servidores virtuais devem entregar o tráfego à um único servidor web e também possuir a opção de distribuir as sessões/conexões entre os servidores web do Server Pool.
- 4.7.10 Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do Server Pool.
- 4.7.11 Permitir teste de disponibilidade de servidor web através do método TCP.
- 4.7.12 Permitir teste de disponibilidade de servidor web através do método ICMP ECHO_REQUEST (ping).
- 4.7.13 Permitir teste de disponibilidade de servidor web através do método TCP Half Open.
- 4.7.14 Permitir teste de disponibilidade de servidor web através do método HTTP.
- 4.7.15 Permitir teste de disponibilidade de servidor web através do método HTTPS.
- 4.7.16 Nos testes de disponibilidade HTTP e HTTPS, permitir indicar a URL exata a ser testada.
- 4.7.17 Nos testes de disponibilidade HTTP e HTTPS, permitir escolher entre os métodos HEAD, GET e POST.
- 4.7.18 Nos testes de disponibilidade HTTP e HTTPS, permitir indicar o nome do campo HTTP "host" a ser testado.
- 4.7.19 Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Host".
- 4.7.20 Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "URL".
- 4.7.21 Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Parâmetro HTTP".
- 4.7.22 Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Referer".
- 4.7.23 Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Endereço IP de Origem".
- 4.7.24 Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Cabeçalho".
- 4.7.25 Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Cookie".
- 4.7.26 Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Valor de campo do Certificado X509".
- 4.7.27 Implementar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados e requisições HTTP sejam respondidas diretamente pela solução.
- 4.7.28 A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por endereço IP de origem.
- 4.7.29 A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando qualquer parâmetro do header HTTP.



- 4.7.30 A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada.
- 4.7.31 A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por cookie – método cookie insert e cookie rewrite.
- 4.7.32 A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por embedded cookie (cookie original mais porção randômica).
- 4.7.33 A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Reescrita de Cookie.
- 4.7.34 A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Cookie Persistente.
- 4.7.35 A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em ASP Session ID.
- 4.7.36 A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em PHP Session ID.
- 4.7.37 A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em JSP Session ID.
- 4.7.38 A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por sessão SSL.
- 4.7.39 A solução deverá ser capaz de enviar código de erro 503 caso o health-check dos servidores estiver desabilitado e/ou o servidor/serviço de retaguarda não estiver responsivo.



ANEXO II

MODELO DE PROPOSTA COMERCIAL

Nome Fantasia:			
Razão Social:			
CNPJ:		Inscrição Estadual:	
Endereço:			Cidade:
Estado:	CEP:	Telefone:	E-mail:

Lote Único: Solução de Firewall de Aplicação WEB

ID	Descrição	Quantidade Aquisição Imediata	Quantidade Registrada	Valor Unitário	Num Parcelas	Total Aquisição Imediata	Total Quantidade Registrada
1.	Virtual Appliance com garantia de 36 meses Marca/ Modelo/Versão:	02	04	Por Appliance	1 (uma)		
2.	Licenciamento da solução, suporte e atualizações do fabricante por 36 meses.	02	04	Mensal por licenciamento	36 (trinta e seis) meses consecutivos		
3.	Serviço de Implantação da solução e configuração de aplicações protegidas.	01	02	Por implantação	1 (uma)		
4.	Serviço de Suporte da solução com Gerenciamento Continuado por 36 meses.	01	02	Mensal por suporte	36 (trinta e seis) meses consecutivos		
Valor Global – Quantidade Registrada ⇨							

Declaramos que tomamos conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto deste Pregão Eletrônico, bem como que dispomos de instalações, aparelhamento e pessoal técnico, suficientes para a realização integral do objeto da mesma.

Declaramos que todas as exigências do edital – inclusive os serviços de garantia, suporte e atualização por 36 (trinta e seis) meses consecutivos – encontram-se contemplados nos preços ofertados.

Prazo de validade da proposta: 90 (noventa) dias.

Localidade, ____ de ____ de ____.

NOME DO REPRESENTANTE LEGAL E ASSINATURA



ANEXO III

**TERMO DE ACEITAÇÃO E AUTORIZAÇÃO EXPRESSA DE
SUBCONTRATAÇÃO**

O ESTADO DA BAHIA, pessoa jurídica de direito público, inscrito no CNPJ/MF sob o nº 13.937.032/0001-60, por intermédio do **TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA**, órgão do Poder Judiciário, inscrito no CNPJ/MF sob o nº 13.100.722/0001-60, com sede e foro nesta cidade de Salvador, Estado da Bahia, na Quinta Avenida, nº 560, Centro Administrativo da Bahia – CAB, representado pela(o) sua(eu) Presidente, **Desembargadora(or)** _____, nos termos das normas constantes da Lei Federal nº 8.666/93, Lei Estadual nº 9.433/05, e conforme as disposições contidas no Processo Licitatório Pregão Eletrônico ___/___, item ___ da SUBCONTRATAÇÃO, vem, por meio deste, conforme requerimento apresentado pela CONTRATADA, no dia ___ de _____ de _____, **AUTORIZAR** a subcontratação do serviço e materiais à empresa _____, para o evento _____, entre os dias ___ e ___ de _____ de _____, que acontecerá no local _____.

Salvador, ___ de _____ de _____.

TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA

Desa.(es.) _____
Presidente



ANEXO IV

MODELO DO TERMO DE CONFIDENCIALIDADE

ANEXO I AO CONTRATO DE
PRESTAÇÃO DE SERVIÇOS QUE ENTRE
SI CELEBRAM, E A

EMPRESA

(Pregão Eletrônico nº xx/xxxx - Processo
nº xxxxxx/xxxxx)

TERMO DE CONFIDENCIALIDADE SOBRE A SEGURANÇA DA INFORMAÇÃO

O ESTADO DA BAHIA, pessoa jurídica de direito público, inscrito no CNPJ/MF sob o nº 13.937.032/0001-60, por intermédio do **TRIBUNAL DE JUSTIÇA DA BAHIA**, órgão do Poder Judiciário, inscrito no CNPJ/MF sob nº 13100722/0001-60, com sede e foro nesta cidade do Salvador, Estado da Bahia, na Quinta Avenida, nº 560, Centro Administrativo da Bahia – CAB, representado por..... adiante denominada simplesmente **CONTRATANTE**, e, do outro lado,..... inscrita no CNPJ sob nº....., doravante designada simplesmente **CONTRATADA**, representada por, inscrito no CPF/MF sob nº, resolvem, tendo em vista o constante do **PA nº** com arrimo nas normas pertinentes da Lei Estadual nº 9.433/05 e, no que couber, na Lei Federal nº 8.666/93 e demais dispositivos legais aplicáveis, e tendo em vista o constante no **PA nº xxxxxx/xxxx**, e sempre que em conjunto referidas como PARTES para efeitos deste TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO, doravante denominado simplesmente TERMO, e,

CONSIDERANDO que, em razão do atendimento à exigência do Contrato Nº ..., celebrado pelas PARTES, doravante denominado CONTRATO, cujo objeto é a....., mediante condições estabelecidas pelo **CONTRATANTE**;

CONSIDERANDO que o presente TERMO vem para regular o uso dos dados, regras de negócio, documentos, informações, sejam elas escritas ou verbais ou de qualquer outro modo apresentada, tangível ou intangível, entre outras, doravante denominadas simplesmente de INFORMAÇÕES, que aNOME DA EMPRESA..... tiver acesso em virtude da execução contratual;

CONSIDERANDO a necessidade de manter sigilo e confidencialidade, sob pena de responsabilidade civil, penal e administrativa, conforme tipificado no art.325 do Decreto – Lei 2.848/1940 (Código Penal Brasileiro), sobre todo e qualquer assunto de interesse do **CONTRATANTE** de que aNOME DA EMPRESA..... tomar conhecimento em razão da execução do CONTRATO, respeitando todos os critérios estabelecidos aplicáveis às INFORMAÇÕES;

O **CONTRATANTE** estabelece o presente TERMO mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA – DO OBJETO



O objeto deste TERMO é prover a necessária e adequada proteção às INFORMAÇÕES do **CONTRATANTE**, principalmente aquelas classificadas como CONFIDENCIAIS, **exemplificadas no tópico 02.13.28 do Termo de Referência – ANEXO I do edital**, em razão da execução do CONTRATO celebrado entre as PARTES.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

- a) As estipulações e obrigações constantes do presente instrumento serão aplicadas a todas e quaisquer INFORMAÇÕES reveladas pelo **CONTRATANTE**;
- b) ANOME DA EMPRESA..... se obriga a manter o mais absoluto sigilo e confidencialidade com relação a todas e quaisquer INFORMAÇÕES que venham a ser fornecidas pelo **CONTRATANTE**, a partir da data de assinatura deste TERMO, devendo ser tratadas como INFORMAÇÕES CONFIDENCIAIS, salvo aquelas prévia e formalmente classificadas com tratamento diferenciado pelo **CONTRATANTE**;
- c) ANOME DA EMPRESA..... se obriga a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que nenhum de seus diretores, empregados e/ou prepostos faça uso das INFORMAÇÕES do **CONTRATANTE**;
- d) O **CONTRATANTE**, com base nos princípios instituídos na Segurança da Informação, zelará para que as INFORMAÇÕES que receber e tiver conhecimento sejam tratadas conforme a natureza de classificação informada pelaNOME DA EMPRESA.....
- e) O **CONTRATANTE** pode, sem aviso prévio, restringir ou bloquear o acesso a Web Sites, serviços da Internet ou download de arquivos e examinar o conteúdo das mensagens de correio eletrônico, arquivos em computadores, cache de navegadores Web, bookmarks, histórico de sites visitados, configurações dos softwares e outras informações armazenadas ou transmitidas pelos seus computadores;
- f) ANOME DA EMPRESA..... obriga-se a preservar o sigilo das senhas das contas dos usuários, não cedê-las nem facilitar a sua descoberta, sob qualquer pretexto, bem como não utilizar contas e senhas pertencentes a outros servidores.

CLÁUSULA TERCEIRA – DAS LIMITAÇÕES DA CONFIDENCIALIDADE

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

- a) Sejam comprovadamente de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão das PARTES;
- b) Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
- c) Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as PARTES cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES ADICIONAIS

- a) ANOME DA EMPRESA..... se compromete a utilizar as INFORMAÇÕES reveladas exclusivamente para os propósitos da execução do CONTRATO;



- b) ANOME DA EMPRESA..... se compromete a não efetuar qualquer cópia das INFORMAÇÕES sem o consentimento prévio e expresso do **CONTRATANTE**;
- b1) O consentimento mencionado na alínea “b”, entretanto, será dispensado para cópias, reproduções ou duplicações para uso interno das PARTES;
- c) ANOME DA EMPRESA..... se compromete a cientificar seus diretores, empregados e/ou prepostos da existência deste TERMO e da natureza confidencial das INFORMAÇÕES do **CONTRATANTE**;
- d) ANOME DA EMPRESA..... deve tomar todas as medidas necessárias à proteção das INFORMAÇÕES do **CONTRATANTE**, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo **CONTRATANTE**;
- e) Cada PARTE permanecerá como única proprietária de todas e quaisquer INFORMAÇÕES eventualmente reveladas à outra parte em função da execução do CONTRATO;
- f) O presente TERMO não implica a concessão, pela parte reveladora à parte receptora, de nenhuma licença ou qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito relativo à propriedade intelectual;
- g) Os produtos gerados na execução do CONTRATO, bem como as INFORMAÇÕES repassadas àNOME DA EMPRESA....., são única e exclusiva propriedade intelectual do **CONTRATANTE**;
- h) ANOME DA EMPRESA..... **firmará acordos por escrito com cada um de seus empregados e consultores ligados direta ou indiretamente ao CONTRATO, cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente instrumento, entregando uma via ao CONTRATANTE**;
- i) ANOME DA EMPRESA..... obriga-se a não tomar qualquer medida com vistas a obter, para si ou para terceiros, os direitos de propriedade intelectual relativos aos produtos gerados e às INFORMAÇÕES que venham a ser reveladas durante a execução do CONTRATO;
- j) ANOME DA EMPRESA..... se compromete a envidar todos os esforços para preservar a confidencialidade das informações, adotando práticas de trabalho seguras quanto ao manuseio, armazenamento, transporte, impressão, transmissão e, quando for o caso, destruição de informações pertencentes ao **CONTRATANTE**;
- k) ANOME DA EMPRESA..... se compromete a estar engajado na promoção de Segurança da Informação, incorporando as suas recomendações às atividades diárias do trabalho;
- l) ANOME DA EMPRESA..... se compromete a notificar à Área de Segurança da Informação do **CONTRATANTE** em caso de divulgação ou suspeita de divulgação, acidental ou intencional, de informações pertencentes ao **CONTRATANTE**, bem como a descoberta de fragilidades de sistemas ou processos que possam propiciar a quebra de confidencialidade, disponibilidade ou integridade das informações.

CLÁUSULA QUINTA – DO RETORNO DE INFORMAÇÕES

Todas as INFORMAÇÕES reveladas pelas PARTES permanecem como propriedade exclusiva da parte reveladora, devendo a esta retornar imediatamente assim que por ela requerido, bem como todas e quaisquer cópias eventualmente existentes.

CLÁUSULA SEXTA – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irreatável, permanecendo em vigor desde a data de sua assinatura, até 5 (cinco) anos após o término do Contrato, e persiste após o término da atividade, mudança de função ou de encerramento do vínculo empregatício com a empresa.



CLÁUSULA SÉTIMA – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO firmado entre as PARTES. Neste caso, aNOME DA EMPRESA....., estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial.

CLÁUSULA OITAVA - DAS DISPOSIÇÕES GERAIS

- a) Este TERMO constitui vínculo indissociável ao CONTRATO, que é parte independente e regulatória deste instrumento;
- b) O presente TERMO constitui acordo entre as PARTES, relativamente ao tratamento de INFORMAÇÕES, principalmente as CONFIDENCIAIS, aplicando-se a todos e quaisquer acordos futuros, declarações, entendimentos e negociações escritas ou verbais, empreendidas pelas PARTES em ações feitas direta ou indiretamente;
- c) Surgindo divergências quanto à interpretação do pactuado neste TERMO ou quanto à execução das obrigações dele decorrentes, ou constatando-se nele a existência de lacunas, solucionarão as PARTES tais divergências, de acordo com os princípios da legalidade, da equidade, da razoabilidade, da economicidade, da boa-fé, e, as preencherão com estipulações que deverão corresponder e resguardar as INFORMAÇÕES do **CONTRATANTE**;
- d) O disposto no presente TERMO prevalecerá sempre em caso de dúvida, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos legais conexos relativos à confidencialidade de INFORMAÇÕES;
- e) A omissão ou tolerância das PARTES, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo.

CLÁUSULA NONA - DO FORO

O **CONTRATANTE** elege o foro de Salvador-BA, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, é assinado o presente TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO, pelaNOME DA EMPRESA....., sendo em 2 (duas) vias de igual teor e um só efeito.

Salvador, _____ de _____ de ____.

Nome

Diretor

.....NOME DA EMPRESA.....



ANEXO V

MODELO DO TERMO DE DESIGNAÇÃO DE PREPOSTO

(Logomarca da empresa em papel timbrado)

Em atenção ao disposto no **Contrato nº. .../XXXX**, apresentamos o Senhor _____ portador do RG nº _____, inscrito no CPF/MF nº _____, como representante desta empresa, com poderes para responder, perante ao Tribunal de Justiça da Bahia, pela entrega de appliances virtuais de firewall de aplicações web (WAF – Web Firewall Application), incluindo serviço de implantação da solução e serviços continuados de garantia, licenciamento, suporte e gerenciamento até o total cumprimento das obrigações assumidas contratualmente, bem como, para receber as instruções dadas ou formalizadas por escrito e/ou e-mail pelo representante do TJBA.

Salvador, ____ de _____ de ____.

(Nome, identidade e assinatura do Representante da Empresa)