Termo de Referência

Sumário

1. OBJETO

Aquisição de solução de Controle de Entrega de Aplicações (ADC) com funcionalidades de firewall de aplicação web (WAF) e balanceamento de carga (Load Balance), com suporte técnico e garantia inclusos no licenciamento pelo período de 36 meses e Serviço de implantação.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. Contextualização e justificativa da contratação

O Poder Judiciário De Mato Grosso do Sul (PJMS) possui diversas aplicações web em sua atividade que precisam ser protegidos contra vulnerabilidades e ataques cibernéticos, como o Portal E-SAJ, sítio institucional, intranet, sistemas de licitações, sistema de atendimento ao usuário, entre outros.

Para enfrentar o crescimento exponencial dos ataques cibernéticos é essencial adotar tecnologias aprimoradas capazes de suportar a demanda e fornecer segurança aos serviços disponibilizados aos usuários internos e externos, como a adoção de uma solução de solução de firewall de aplicação Web (WAF).

Isso irá contribuir na confidencialidade, disponibilidade e integridade dos dados armazenados na infraestrutura tecnológica do Poder Judiciário e melhorar o acesso aos serviços para os usuários.

Ademais, recentemente têm ocorrido diversos ataques cibernéticos contra entidades públicas e privadas, o que motivou o Conselho Nacional de Justiça (CNJ) a recomendar que os órgãos do Poder Judiciário se preparassem para lidar com essas ameaças. Em 2021 o CNJ estabeleceu a Resolução Nº 396/2021 que determina que os Tribunais adotem medidas de segurança cibernética e proteção de dados pessoais para prevenir e combater ataques cibernéticos e minimizar os possíveis danos que tais ataques possam causar às atividades jurisdicionais dos Tribunais brasileiros.

Assim sendo, a contratação de recursos de segurança da informação em geral, e especificamente de uma solução de firewall de aplicação, visa dotar a infraestrutura do PJMS de meios tecnológicos efetivos para proteção das aplicações disponibilizadas na

modalidade web em conformidade tanto com as boas práticas de segurança cibernética como também em conformidade com as resoluções do CNJ neste campo.

2.2. Itens que compõem a solução de TIC

ITEM	ESPECIFICAÇÃO	MÉTRICA	CATMAT/CATSER
01	Solução de controle de entrega de aplicações (ADC) com funcionalidades de firewall de aplicação web (WAF) e balanceamento de carga (Load Balance) com suporte técnico e garantia inclusos no licenciamento pelo período de 36 meses.	UN	33904011
02	Serviço de implantação da solução	SV	33904005

2.3. Resultados e benefícios a serem alcançados

2.3.1. A solução trará como benefício a ampliação da proteção de dados do PJMS, permitindo:

a. Proteger aplicações web disponibilizadas pelo PJMS, tanto para o público interno quanto o público externo, contra acessos que busquem realizar ações indevidas (ataques) que configurem a perda da segurança da informação (confidencialidade, autenticidade e disponibilidade);

b. Promover maior eficiência no acesso às aplicações web disponibilizadas pelo PJMS através da técnica de balanceamento de carga;

c. Balanceamento de acessos externos para os servidores que hospedam sistemas web considerados críticos para as atividades institucionais, como e-SAJ.

2.4. Alinhamento aos instrumentos de planejamento do PJMS

2.4.1. Atender ao(s) seguinte(s) Objetivo(s) Estratégico(s) do Plano Estratégico 2021-2026 do PJMS:

Alinhamento ao Planejamento Estratégico do PJMS	
ID	**Objetivos Estratégicos**
13	Fortalecer a governança de tecnologia da informação e comunicação e de proteção de dados.
Alinhamento ao PDTIC 2023-2024	
OE7	Promover e Fortalecer a Segurança da Informação e a Gestão de Dados

2.5. **Dos Estudos Técnicos Preliminares.**

2.5.1. Os Estudos Técnicos Preliminares, que fundamentam, detalhadamente, todo o rol de exigências, necessidades, quantitativos e considerações deste Termo de referência estão no processo eletrônico de número 159.943.0013/2023.

2.6. **Relação da demanda prevista para atender as necessidades do PJMS.**

ITEM	ESPECIFICAÇÃO	TIPO	MÉTRICA	QTD
01	Licenciamento de Controlador de Entrega de Aplicativos (ADC) virtual (Appliance virtual) com recursos de Firewall de Aplicação Web (WAF) e Balanceamento de carga (Load Balance) com garantia e suporte técnico do fabricante por 36 meses.	Licença	UN	02
02	Serviços de implantação com repasse de conhecimento	Serviço	SV	01

2.7. **Análise de Mercado**

2.7.1. Sobre a análise de mercado, com os levantamentos e detalhamento da solução e seu respectivo valor estimado, foi documentada nos Estudos

Técnicos Preliminares da etapa de Planejamento da Contratação do processo nº 159.943.0013/2023.

2.8. Estimativa de preços

2.8.1. Para o valor estimado total da contratação será considerada a pesquisa de preço realizada pela Coordenadoria de Compras.

2.8.2. A estimativa de preços informada no Estudo Técnico Preliminar refere-se a uma pesquisa prévia inicial, e não servirá como base para reserva orçamentária.

2.9. Classificação Orçamentária

2.9.1. A presente aquisição ocorrerá por conta da Ação/localizador/Funcional Programática: FP: 02.126.0003.2045.0002 - Segurança da Informação.

2.10. Impacto Ambiental

2.10.1. A CONTRATADA deve demonstrar compromisso com as diretrizes de sustentabilidade do TJMS, adaptando suas operações para cumprir com os objetivos de redução do consumo de papel e gastos com telefonia.

2.10.2. Todos os relatórios, documentos, e comunicações relacionadas aos serviços devem, preferencialmente, ser enviados em formato digital, como arquivos PDF, evitando a impressão desnecessária de papéis.

2.10.3. A CONTRATADA deve priorizar mecanismos de comunicação eletrônicos, como e-mails e mensagens instantâneas, reduzindo a necessidade de comunicação via telefonia tradicional.

2.10.4. A CONTRATADA deve instruir os seus colaboradores quanto à necessidade de racionalização de recursos no desempenho de suas atribuições, bem como das diretrizes de responsabilidade ambiental adotadas pelo Tribunal.

2.11. **Conformidade técnica e legal**

2.11.1. A contratação como um todo deve estar em conformidade com a lei geral de licitações, Lei no 14.133/2021, com a Lei de Acesso à Informação e com os normativos vigentes que regem contratação de bens e serviços de TI do PJMS.

3. ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO

O detalhamento e exigências específicas para a solução estão descritas no **ANEXO I – ESPECIFICAÇÃO DETALHADA DO OBJETO.**

4. REQUISITOS DA CONTRATAÇÃO

4.1. **Apresentação de documentação técnica**

4.1.1. Para a comprovação do atendimento das especificações técnicas, a LICITANTE deverá apresentar documento detalhando as informações, local, site, páginas, documento, etc, necessários para aferição e atendimento de todos os itens da especificação técnica, ou seja, deverá apresentar uma espécie de índice, indicando o item, o documento que atende a especificação (nome do mesmo), O local onde está disponibilizado o documento (URL, Site, ou outro disponibilizado de forma digital), a página, e o texto que comprova o atendimento ao item.

4.1.2. Devido às especificidades do sistema e seu método de envio/carregamento de documentos, recomendamos o envio da documentação com no mínimo 2 dias antes ao momento de início do certame.

4.1.3. A omissão de comprovação técnica da regularidade do item ofertado frente às exigências técnicas, através da documentação oficial/declaração do fabricante da solução, fundamentará a possibilidade de

questionamento por parte da equipe técnica para atestar a conformidade do objeto ofertado com o item homologado.

4.1.4. A proposta será desclassificada quando:

a. Não for possível realizar a devida identificação, validação e comprovação das características técnicas exigidas, por meio da documentação oficial apresentada pelo Licitante.

b. A proposta ou a documentação técnica demonstrarem características insuficientes / inferiores às exigidas ao item.

4.2. **Das Entregas, Prazos, Notas Fiscais e Condições de Recebimento e Pagamento dos Itens**

4.2.1. Deverá ser realizada, nas dependências da CONTRATANTE ou por videoconferência, reunião preparatória com o intuito de esclarecer obrigações contratuais, apresentação do preposto e entrega dos termos de compromisso e confidencialidade, no prazo de 15 (quinze) dias, contados da data da assinatura do Contrato;

4.2.2. A entrega da solução instalada e configurada deverá ser concluída em até 60 (sessenta) dias após a assinatura do contrato;

4.2.3. O início da implantação da solução deverá iniciar em até 30 (trinta) dias após a assinatura do contrato;

4.2.4. A passagem de conhecimento deverá ser concluída em até 70 (setenta) dias contados a partir da assinatura do contrato;

4.2.5. Ao concluir a implantação, a CONTRATADA deverá encaminhar uma declaração de implantação da solução e relatório final de implantação (modelos - anexo I) para a equipe de fiscalização, que terá 05 (cinco) dias uteis para avaliar e emitir o Termo de Recebimento Definitivo.

4.2.6. O pagamento será realizado, em até 10 (dez) dias úteis, após o recebimento definitivo do objeto pela Equipe de fiscalização.

4.2.7. A CONTRATADA deve emitir nota fiscal contendo no campo descrição ou observação, no mínimo as seguintes informações: número do contrato, número do empenho, fabricante, produto, identificação das licenças (Part Numbers) e prazo de garantia.;

a. Havendo erro no documento de cobrança, este será devolvido para que a CONTRATADA tome as medidas necessárias, passando o prazo para pagamento a ser contado a partir da data de sua reapresentação;

4.2.8. A nota fiscal/fatura deverá ser encaminhada para o e-mail sti.notas@tjms.jus.br.

4.3. **Da implantação da solução e repasse de conhecimento**

4.3.1. A CONTRATADA deve fornecer um plano de implantação detalhado, incluindo cronogramas, etapas, responsabilidades e recursos necessários;

4.3.2. O cronograma deverá ser previamente acordado com a equipe técnica da área de cibersegurança da STI, considerando a disponibilidade e o tempo necessário para realização de todos os trâmites necessários à execução da instalação, incluindo o tempo necessário para obtenção das autorizações de acesso;

4.3.3. A CONTRATADA deverá disponibilizar um gerente de projetos, com experiência comprovada em projetos similares, para gerenciamento e execução dos serviços de implantação da solução;

4.3.4. O serviço de implantação consiste na instalação, customização e configuração da solução contratada em perfeitas condições de operação, de forma integrada ao ambiente da CONTRATANTE, devendo contemplar, no mínimo:

a. A CONTRATADA deverá efetuar instalação e configuração realizada de acordo com as recomendações do fabricante;

b. A CONTRATADA deverá efetuar a instalação dos appliances na infraestrutura indicada pelo CONTRATANTE, onde a configuração

realizada deverá estar em conformidade com as recomendações do fabricante (recommended settings);

c. Atualização de softwares, firmwares e drivers que compõem a solução;

d. Aplicação das licenças necessárias à solução entregue;

e. Testes da solução, incluindo testes de failover;

f. Documentação do ambiente configurado e instalado (AS BUILT).

4.3.5. O prazo para início do serviço é de 30 dias após a assinatura do contrato;

4.3.6. Os serviços de instalação e configuração deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante em seus manuais de instalação e configuração ou artigos técnicos.

4.3.7. A solução deverá ser entregue com todas as funcionalidades, recursos, componentes, acessórios, softwares e licenciamentos necessários para atendimento das especificações técnicas.

4.3.8. A solução deverá ser configurada em alta disponibilidade;

4.3.9. Todas as informações necessárias à implantação, que deverão ser utilizadas necessárias à perfeita configuração, implementação da solução, e funcionamento da solução serão fornecidas pelo CONTRATANTE.

4.3.10. A CONTRATADA deverá providenciar um profissional com a expertise e conhecimento no produto, para garantir a conformidade da instalação e a configuração dos equipamentos e softwares que compõem a solução.

4.3.11. Os serviços poderão ser executados presencialmente no ambiente da Secretaria de Tecnologia da Informação ou **remotamente**;

4.3.12. Deverá ser realizada a configuração da solução na rede, com recebimento automático de novas assinaturas e demais atualizações de segurança periodicamente, conforme orientações do fabricante;

4.3.13. Se compatível, deverá ser realizada a integração da solução com o gerenciamento centralizado e envio de registros de eventos (SIEM);

4.3.14. As operações poderão ser assistidas por servidor da CONTRATANTE;

4.3.15. Após a implantação, o ambiente deverá ser monitorado pelo prazo mínimo de 2 (duas) horas corridas, observando as condições de funcionamento e performance da solução, possibilitando troubleshooting em caso de problemas ou não conformidades na operação, a ser realizada no final de semana ou fora do horário de expediente padrão do PJMS;

4.3.16. Após este período, faz necessário o acompanhamento por, no mínimo, mais 03 (três) dias com a solução em pleno funcionamento durante dias de trabalho normal, pelo mesmo técnico que participou do processo de implementação. Com objetivo de correção de eventuais problemas e verificações periódicas do desempenho, bloqueios e possíveis mudanças no ambiente devido ao aumento de carga, diferenças de funcionamento ou situações não previstas.

4.3.17. Ao concluir a implantação, a CONTRATADA deverá encaminhar uma declaração de implantação da solução e relatório final de implantação (modelos - anexo I) para a equipe de fiscalização.

4.3.18. A CONTRATADA, deverá disponibilizar passagem de conhecimento em quantidade suficiente para abranger todos os assuntos operacionais da solução, com carga horária mínima de 15 horas, a serem ministradas no período da tarde. Deverá ser do tipo presencial ou remoto, com aulas ao vivo em língua portuguesa. O material didático poderá ser fornecido em formato digital em língua inglesa ou portuguesa.

4.3.19. Deverá cobrir, no mínimo, os seguintes assuntos:

a. Arquitetura e plataforma;
b. Configuração inicial;
c. Publicação de aplicações;
d. Balanceamento de carga;
e. Aplicação de políticas de Web Application Firewall;

f. Métodos de autenticação;
g. Monitoramento e relatórios;
h. Demais assuntos pertinentes à solução.

4.4. **Da manutenção da solução (suporte técnico e garantia)**

4.4.1. A vigência da garantia técnica de 36 (trinta e seis) meses começará a contar a partir da entrega das licenças.

4.4.2. A CONTRATADA é responsável junto à CONTRATANTE pelo serviço de suporte técnico e poderá ser prestado pela CONTRATADA ou pelo FABRICANTE da solução.

4.4.3. As solicitações de suporte técnico deverão ser feitas via chamada telefônica local, chamada telefônica gratuita (0800), e-mail, ou site WEB à fabricante/contratada. Sendo possível registrar, no mínimo:

a. descrição da solicitação;
b. nome e contato do responsável pela solicitação do serviço, por parte da CONTRATANTE;
c. nível de severidade do chamado, de acordo com a tabela a seguir:

Grau de severidade	Descrição
Alta	Serviço urgente. Existe alto impacto no uso da solução no ambiente de produção e há o comprometimento do funcionamento dos trabalhos da organização. Não há solução de contorno.
Média	Serviço em que existe alto impacto no uso da solução no ambiente de produção, mas não há comprometimento do funcionamento por completo dos trabalhos da organização. Pode haver solução de contorno.

Baixa	Serviço em que existe baixo impacto no uso da solução no ambiente de produção e não há comprometimento nos trabalhos da organização; Esclarecimento de dúvidas sobre as funcionalidades do software; Implantação de novas funcionalidades.

Tabela 1 – Graus de severidade para chamados de suporte técnico.

4.4.4. Os chamados serão centralizados na central de atendimento, independentemente da plataforma pelo qual foram abertos.

4.4.5. A definição da gravidade do chamado de suporte técnico será prerrogativa da CONTRATANTE.

4.4.6. A prestação de Serviço de Suporte Técnico deverá ser 24x7 atendendo todas as demandas de suporte em português.

4.4.7. O suporte não poderá limitar uma quantidade máxima de chamados abertos pela contratada, independentemente do nível de criticidade;

4.4.8. Os prazos para conclusão do atendimento para os chamados de assistência técnica serão os definidos na tabela a seguir:

Grau de severidade	Prazo para conclusão
Alta	8 horas
Média	6 dias úteis
Baixa	10 dias úteis

Tabela 2 – Prazo de conclusão das requisições de suporte técnico em função da severidade.

4.4.9. Os tempos de atendimento serão contados a partir do recebimento do chamado. No caso da contagem em dias, a contagem será efetuada dia a dia, incluindo o primeiro e o último dia.

4.4.10. O cálculo de dias úteis será realizado com base na diferença entre a data/hora final e a data/hora inicial da contagem de prazo, considerando apenas os dias úteis e o horário de funcionamento da CONTRATANTE. Serão excluídos da contagem sábados, domingos e feriados.

4.4.11. Para os casos em que a CONTRATADA depender de Informações técnicas do CONTRATANTE para atendimento do chamado, o prazo para resolução do chamado (SLA), será acrescido do tempo que a CONTRATANTE levou para apresentar as informações solicitadas.

4.4.12. O período para contato da CONTRATADA com a CONTRATANTE, para apresentação das informações adicionais e necessárias, será de segunda a sexta feira, das 12 às 19 horas (horário local da CONTRATANTE em dias úteis).

4.5. **Requisitos de segurança da informação**

4.5.1. A CONTRATADA deverá aderir rigorosamente às diretrizes da Política de Segurança de Informação do PJMS, Resolução Nº 239, de 17 de março de 2021 e Portaria Nº 774, de 03 de agosto de 2015, que define o uso de cláusulas de Confidencialidade nos contratos firmados pelo Poder Judiciário. Isso inclui os normativos, padrões e processos internos.

4.5.2. A CONTRATADA deverá adotar critérios adequados para o processo seletivo dos profissionais, com o propósito de evitar a incorporação de pessoas com características e/ou antecedentes que possam comprometer a segurança ou credibilidade do PJMS.

5. DA LICITAÇÃO

5.1. **Da Natureza do objeto**

5.1.1. Esta contratação tem natureza de **serviço comum**, de caráter continuado e sem fornecimento de mão-de-obra em regime de dedicação exclusiva.

5.2. **Do Parcelamento e adjudicação do objeto**

5.2.1. Será realizado uma única licitação, com todo o objeto adjudicado a um único licitante, mas havendo permissão para que a licitante vencedora subcontrate outras empresas, com o objetivo de agilizar a resolução de problemas, desde que sejam empresas autorizadas pela fabricante da solução.

5.3. **Da Modalidade e tipo de licitação**

5.3.1. Para fins de aplicação do disposto no art. 29, combinado com o Art. 33, inciso I da Lei nº 14133/2021, considerando que os itens/serviços ora propostos: (a) tem um padrão de desempenho e qualidade; (b) tal padrão de desempenho e qualidade pode ser objetivamente definido em edital; e (c) tal objetividade resulta de especificações usuais no mercado; compreende-se que esta licitação deve ser realizada na modalidade de **Pregão**, na sua forma eletrônica, com julgamento pelo critério de **menor preço**, e o uso do modo "**Aberto**" sem indicação de diferença mínima entre os lances.

5.4. **Critérios de qualificação técnica para habilitação**

5.4.1. Será requerida das empresas licitantes, para fins de habilitação, a comprovação de aptidão para a implantação de solução de balanceamento e firewall de aplicações web (WAF).

5.4.2. O documento de comprovação deverá constar que a licitante realizou a implantação da solução ofertada e prestou serviço de suporte técnico por, no mínimo, 12 (doze) meses.

a. É vedado o somatório de atestados, condição que visa garantir a adequada aptidão do fornecedor em relação à solução, tal qual é indispensável a comprovação de que este já executou os respectivos serviços de implantação e suporte em solução de Balanceamento de Carga e Firewall de Aplicação Web por, no mínimo, 12 (doze) meses. Tal critério oferece uma visão mais clara da capacidade operacional do licitante em projetos de longa duração, minimizando riscos para o TJMS.

5.4.3. Para comprovação, será aceita, cópia(s) de contrato(s), atestado(s) ou declaração(ões) de órgão ou entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou empresa privada emitidos em favor da LICITANTE.

5.4.4. Não serão considerados os atestados emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente ou que tenham pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da proponente;

5.4.5. A LICITANTE deve disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados ofertados na presente licitação, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, Notas Fiscais/Faturas, Notas de Empenho, endereço atual da empresa ou órgão e local em que foram prestados os serviços, sendo que estas e outras informações complementares poderão ser requeridas mediante diligência.

5.5. **Participação de consórcios**

5.5.1. Fica vedada a participação de pessoas jurídicas reunidas em consórcio para participação do certame da presente contratação.

5.5.2. A ausência de consórcio não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os

requisitos de habilitação da contratação. Nesses casos, o CONTRATANTE, a fim de aumentar o número de participantes, admite a formação de consórcio. O que não é o caso do referido objeto.

6. ASPECTOS CONTRATUAIS

6.1. Vigência do contrato

6.1.1. O prazo de vigência contratual será de 36 (trinta e seis) meses, podendo ser prorrogado até o limite máximo permitido pela legislação vigente.

6.1.2. A prorrogação do contrato será precedida de um atestado emitido pela equipe responsável pela gestão e fiscalização do contrato, confirmando que as condições e os preços continuam sendo vantajosos para o CONTRATANTE.

6.2. Garantia de execução contratual

6.2.1. Não será exigida garantia de execução contratual.

6.3. Subcontratação

6.3.1. É permitido à CONTRATADA a subcontratação parcial para a execução dos serviços de implantação e Suporte Técnico, desde que devidamente aprovado pela Equipe de Gestão da Contratação.

6.4. Obrigações da CONTRATADA

6.4.1. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

6.4.2. Indicar formalmente preposto apto a representá-la junto ao CONTRATANTE, que deverá responder pela fiel execução do contrato;

6.4.3. Efetuar a entrega da solução em perfeitas condições, conforme especificações, prazo e local constantes neste Termo de Referência,

acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: fabricante, produto, identificação das licenças (Part Numbers) e prazo de garantia.

6.4.4. Todos os custos de pessoal para efetuar a implementação da solução, tais como passagens áreas ou terrestres, hospedagem, alimentação, deslocamentos e demais custos, serão de responsabilidade da CONTRATADA;

6.4.5. Guardar sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do objeto contratual.

6.4.6. Participar de reuniões (inicial, periódica, de transição contratual e/ou final) convocadas pelo CONTRATANTE.

6.4.7. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

6.4.8. Comunicar ao CONTRATANTE sobre qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários.

6.4.9. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pela equipe de fiscalização, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

6.4.10. Substituir qualquer de seus profissionais cuja qualificação, atuação, permanência ou comportamento durante a execução do objeto forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina do órgão ou ao interesse do serviço público por outro de qualificação igual ou superior, sempre que exigido pelo contratante;

6.4.11. Reparar quaisquer danos diretamente causados ao CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou

empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pelo CONTRATANTE;

6.4.12. Ter pleno conhecimento de todas as condições, características, procedimentos e peculiaridades do objeto contratado, não podendo alegar, posteriormente, desconhecimento acerca do contrato.

6.4.13. Cumprir e garantir que seus profissionais estejam aderentes à Política de Segurança da Informação do PJMS e demais normas que disciplinam o uso dos recursos tecnológicos e de informação do PJMS;

6.4.14. Entregar ao PJMS toda e qualquer documentação produzida decorrente da prestação de serviços objeto desta licitação, bem como ceder, em caráter definitivo e irrevogável, o direito patrimonial e a propriedade intelectual dos resultados produzidos durante a vigência do contrato e eventuais aditivos. Entende-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, fontes dos códigos dos programas em qualquer mídia, páginas na Intranet e documentação, em papel ou em qualquer forma ou mídia;

6.4.15. Prestar, no prazo fixado pelo CONTRATANTE, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

6.4.16. Fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso;

6.4.17. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários de até 25% (vinte e cinco por cento) do valor inicial do contrato.

6.5. **Obrigações da CONTRATANTE**

6.5.1. Prestar as informações e os esclarecimentos solicitados pela CONTRATADA para a fiel execução do contrato;

6.5.2. Esclarecer à CONTRATADA como serão realizados os procedimentos operacionais/administrativos para a execução e gestão do contrato.

6.5.3. Designar responsáveis para a gestão e fiscalização do objeto contratual.

6.5.4. Aplicar as sanções e penalidades contratuais cabíveis, assegurando à CONTRATADA o contraditório e a ampla defesa.

6.5.5. Promover, se necessário, reuniões (inicial e periódica) devidamente registradas em ATA, para esclarecimento das obrigações contratuais e avaliação da qualidade da execução contratual.

6.5.6. Efetuar o pagamento à CONTRATADA, de acordo com as condições de preço e prazo, ante ateste das notas fiscais, observados indicadores e glosas estabelecidos neste Termo de Referência.

6.6. **Mecanismos formais de comunicação**

6.6.1. Toda a comunicação entre o CONTRATANTE e a CONTRATADA deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação.

6.6.2. A comunicação se dará por e-mail, reuniões virtuais (gravadas), ofícios, telefonemas, e outros correlatos que possam ficar registrados.

6.6.3. Os emissores de comunicações formais, por parte do CONTRATANTE, serão os membros da equipe de fiscalização.

6.6.4. O destinatário de comunicações formais será a figura do preposto da CONTRATADA.

6.7. **Fiscalização e acompanhamento do contrato**

6.7.1. O acompanhamento e a fiscalização da execução do Contrato serão realizados por fiscais e gestores da CONTRATANTE, especialmente designados pelo responsável do órgão:

6.7.2. Gestor do Contratação: Assessor Técnico da Secretaria de Tecnologia da Informação: Rodrigo Cavalari Ferreira Brandão;

6.7.3. Fiscais da Contratação: Coordenador de Segurança da Informação, servidor Luís Otávio Lima Júlio

6.8. **Reajuste**

6.8.1. Os preços poderão ser reajustados, quando e se for o caso, a cada 12 (doze) meses, contado da data do orçamento estimado ou, nos reajustes subsequentes ao primeiro, da data de início dos efeitos financeiros do último reajuste ocorrido, mediante requerimento da CONTRATADA, com base na variação do Índice de Custo da Tecnologia da Informação (ICTI) ou outro que vier a substituí-lo.

6.8.2. A revisão do preço contratual será provocada pela CONTRATADA mediante a apresentação de planilha com demonstração analítica da variação dos componentes dos custos do contrato no período;

6.9. **Direitos de propriedade intelectual**

6.9.1. A CONTRATADA cederá ao CONTRATANTE, nos termos do artigo 93 da lei n. 14133/21, concomitante com o art. 4º, da Lei n. 9609/98, o direito patrimonial e a propriedade intelectual em caráter definitivo dos resultados produzidos em consequência da execução deste objeto.

6.9.2. Entendendo-se por resultados quaisquer estudos, relatórios, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas,

roteiros, tutoriais e qualquer outra documentação produzida no escopo da presente contratação, em papel ou em mídia eletrônica.

6.10. **Sanções Técnicas e de Acordo de Serviço**

6.10.1. A CONTRATADA ficará sujeita, com fundamento nos arts. 155 a 163 da Lei nº 14.133, de 2021, no caso de atraso injustificado, assim considerado pela Administração, de execução parcial ou inexecução de obrigações assumidas, sem prejuízo das responsabilidades civil e criminal, assegurada prévia e ampla defesa, às seguintes sanções:

a. Advertência, em caso de faltas ou descumprimentos de regras contratuais que não causem prejuízo ao CONTRATANTE;
b. Multa;
c. suspensão temporária para licitar e impedimento para contratar com a CONTRATANTE;
d. declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, nos termos da lei.

6.10.2. Ocorrendo atraso injustificado ou com justificativa não aceita pela CONTRATANTE na entrega da solução, à CONTRATADA será imposta multa calculada sobre o valor do Contrato, de acordo com a seguinte tabela:

DIAS DE ATRASO	ÍNDICE DE MULTA	DIAS DE ATRASO	ÍNDICE DE MULTA	DIAS DE ATRASO	ÍNDICE DE MULTA
1	0,1%	**15**	2,0%	**29**	5,7%
2	0,2%	**16**	2,2%	**30**	6,0%
3	0,3%	**17**	2,4%	**31**	6,4%
4	0,4%	**18**	2,6%	**32**	6,8%
5	0,5%	**19**	2,8%	**33**	7,2%
6	0,6%	**20**	3,0%	**34**	7,6%
7	0,7%	**21**	3,3%	**35**	8,0%
8	0,8%	**22**	3,6%	**36**	8,4%

9	0,9%	**23**	3,9%	**37**	8,8%
10	1,0%	**24**	4,2%	**38**	9,2%
11	1,2%	**25**	4,5%	**39**	9,6%
12	1,4%	**26**	4,8%	**40**	10,0%
13	1,6%	**27**	5,1%		
14	1,8%	**28**	5,4%		

Tabela 3 – Índices de multa por dia de atraso na entrega da solução.

6.10.3. Findo o prazo fixado sem que a CONTRATADA tenha concluído a implantação da solução, além da multa prevista, poderá, a critério da CONTRATANTE, ser cancelada, parcial ou totalmente a Nota de Empenho, sem prejuízo de outras sanções legais cabíveis.

6.10.4. Na hipótese de abandono da contratação, a qualquer tempo, ficará a CONTRATADA sujeita à multa de 10% (dez por cento) sobre o valor Contrato, sem prejuízo de outras sanções legais cabíveis.

6.10.5. A CONTRATADA será também considerada em atraso se prestar os serviços em desacordo com as especificações e não corrigir as inconsistências apresentadas dentro do período remanescente do prazo de execução fixado.

6.10.6. Pelo não cumprimento das obrigações contratuais, ou execução insatisfatória dos serviços, omissão e outras faltas não justificadas ou se a CONTRATANTE julgar as justificativas improcedentes, poderão ser impostas à CONTRATADA, ainda, multas por infração cometida, limitadas, em qualquer caso, a 10% (dez por cento), observados, sempre, a reprovabilidade da conduta da CONTRATADA, dolo ou culpa e o disposto no item anterior e levando em conta os princípios da proporcionalidade e razoabilidade, de acordo com a seguinte tabela:

ITEM	INFRAÇÃO	PERCENTUAL

Incidência sobre o valor total do contrato vigente na data da ocorrência do fato		
1.1	Atraso injustificado para início da implantação da solução, de acordo com o prazo estabelecido no item 3.2.3	1%
1.2	Deixar de realizar a passagem de conhecimento	3%
1.3	Não executar, quando solicitado, Plano de Transição entre contratos definido pela CONTRATANTE	1,5%
1.4	Deixar de apresentar o Termo de Compromisso e Termo de Confidencialidade	0,2%
1.5	Deixar de cumprir quaisquer das obrigações pactuadas ou previstas em lei, não previstas nesta Tabela de Multas, por ocorrência.	0,5%
Incidência sobre o valor do serviço de suporte técnico (quando apresentado na proposta) ou 50% do valor total do contrato.		
1.6	Deixar de atender solicitação de suporte técnico com severidade **ALTA** dentro do prazo, sem justificativa aceita pela CONTRATANTE, nos termos do item 3.4.8 Por ocorrência..... Por dia de atraso.....	 5% 2%
1.7	Deixar de atender solicitação de suporte técnico com severidade **MEDIA** dentro do prazo, sem justificativa aceita pela CONTRATANTE, nos termos do item 3.4.8 Por ocorrência..... Por dia de atraso.....	 2% 1%
1.8	Deixar de atender solicitação de suporte técnico com severidade **BAIXA** dentro do prazo, sem justificativa aceita pela CONTRATANTE, nos termos do item 3.4.8 Por ocorrência..... Por dia de atraso.....	 1% 0,5%

Tabela 4 – percentual de multa por infração.

6.10.7. Em qualquer hipótese de aplicação de sanções administrativas, assegurar-se-á o direito ao contraditório e à ampla defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

7. APROVAÇÃO E ASSINATURA

Campo Grande, 15 de março de 2024.

Equipe de Planejamento da Contratação:

Integrante(s) Demandante(s)	Integrante(s) Técnico(s)	Integrante(s) Administrativo(s)
Fernando Monteiro Duarte	Anselmo Shidi Toyota Dheyfesson de Souza Pinheiro	Henrique de Carvalho Correa Chaves

De Acordo:

Liriane Aparecida da Silva Nogueira
Diretora da Secretaria de Tecnologia da Informação

8. ANEXOS

ANEXO I Especificação detalhada do objeto

1. Considerações gerais

1.1. A solução não deve estar listada como “End of Sale” e “End of life” até a data de abertura das propostas;

1.2. A solução deve possuir funções de balanceamento de carga e Web Application Firewall, não podendo ser uma solução de NGFW;

1.3. Deve ser fornecido Appliance Virtual, permitindo a instalação em ambiente virtualizado Vmware Vx-Rail, ESXi 7.0 e superior, Hyper-v 2016 e superior;

1.4. Deve estar licenciado para Throughput de no mínimo 10Gbps.

1.5. Deve suportar a criação de no mínimo 14 IPs virtuais, permitindo balancear e redirecionar diversas urls nos mesmos;

1.6. Deve fornecer todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais;

1.7. Deve possuir suporte a IPv4 e IPv6;

2. Suporte e Garantia do produto

2.1. O suporte e garantia deverão ser oferecidos pelo fabricante;

2.2. Deverá ser informado na proposta os termos da garantia técnica e o nível de suporte oferecido pelo fabricante;

2.3. A garantia será prestada com vistas a manter a solução fornecida em perfeitas condições de uso, sem qualquer ônus ou custo adicional para a CONTRATANTE.

2.4. A CONTRATANTE deve ter acesso às bases de conhecimento de solução de problemas e documentos técnicos;

3. Recursos e especificações da solução

3.1. Gerenciamento e Monitoração

3.1.1. Deve ser possível implementar configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento;

3.1.2. Deve ser possível implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

3.1.3. Deve ser possível permitir acesso in-band via SSH;

3.1.4. Deve ser possível manter internamente múltiplos arquivos / versões de configurações do sistema;

3.1.5. Deve ser possível utilizar SCP, FTP, TFTP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;

3.1.6. Deve possuir auto-complementação de comandos na CLI;

3.1.7. Deve possuir interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos appliances;

3.1.8. Deve possuir, no mínimo, três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;

3.1.9. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

3.1.10. Deve ser possível associar aos usuários de bases externas como RADIUS, LDAP e TACACS+ ao nível de acesso;

3.1.11. Deve possuir Interface Gráfica via Web;

3.1.12. A interface Gráfica deve permitir a atualização e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;

3.1.13. Deve suportar o rollback de configuração e imagem;

3.1.14. Deve possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;

3.1.15. Deve possuir configuração de múltiplos syslog servers para os quais o appliance irá enviar as mensagens de syslog;

3.1.16. A interface Gráfica deve permitir a reinicialização do appliance;

3.1.17. Deve ser possível a reinicialização por comando na CLI;

3.1.18. Deve possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;

3.1.19. Deve possuir traps SNMP;

3.1.20. Deve ser possível implementar Debugging: CLI via console e SSH;

3.1.21. Deve possuir suporte a Link Layer Discovery Protocol (LLDP);

3.1.22. Deve ser possível enviar, pelo menos, as seguintes informações via LLDP: Port ID, Port Description, System Name, System Description, Management Address, Port VLAN ID e Link Aggregation;

3.1.23. A Solução deve ter suporte a sFlow, IPFIX ou NetFlow;

3.2. Balanceamento de Carga

3.2.1. Deve suportar todas as aplicações comuns de um Switch Layer 7, como:

a. Server Load-Balancing;

b. Firewall Load-Balancing;

c. Proxy Load-Balancing;

3.2.2. Deve suportar Balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

3.2.3. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é

realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

3.2.4. Deve possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;

3.2.5. Deve possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;

3.2.6. Deve suportar os seguintes métodos de balanceamento:

3.2.7. Round Robin;

3.2.8. Least Connections;

3.2.9. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

3.2.10. Weighted Percentage (peso);

3.2.11. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;

3.2.12. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;

3.2.13. Deve possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

a. Por cookie: inserção de um novo cookie na sessão;

b. Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;

c. Por endereço IP destino;

d. Por endereço IP origem;

e. Por sessão SSL;

f. Através da análise da URL acessada;

g. Através da análise de qualquer parâmetro no header HTTP;

h. Através da análise do SIP Call ID ou Source IP;

i. Através da análise de qualquer informação da porção de dados (camada 7);

3.2.14. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;

3.2.15. A solução deve suportar os seguintes métodos de monitoramento dos servidores reais:

a. Layer 3 – ICMP;

b. Conexões TCP e UDP pela respectiva porta no servidor;

c. Devem existir monitores predefinidos, ou permitir a criação para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, RADIUS, MSSQL, NNTP, LDAP, SMTP, POP3, SIP, SNMP;

3.2.16. Deve possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);

3.2.17. Deve possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;

3.2.18. Deve possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;

3.2.19. Deve possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

3.2.20. Deve possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:

3.2.21. Realizar Network Address Translation (NAT);

3.2.22. Realizar Proteção contra Denial of Service (DoS);

3.2.23. Realizar Proteção contra Syn flood;

3.2.24. Realizar Limpeza de cabeçalho HTTP;

3.2.25. A solução deve permitir o controle da resposta ICMP por servidor virtual;

3.2.26. Deve possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;

3.2.27. Deve possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;

3.2.28. Deve permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6;

3.2.29. Deve possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

3.2.30. Deve permitir definir qual tipo de compressão será habilitada;

3.2.31. Deve possuir capacidade para definir compressão especificamente para certos tipos de objetos;

3.2.32. Deve possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no appliance e as requisições HTTP são enviadas aos servidores sem criptografia;

3.2.33. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e recriptografar o tráfego SSL sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor;

3.2.34. A solução deve possuir a funcionalidade de espelhamento de conexões SSL;

3.2.35. Deve possuir recursos para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado;

3.2.36. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste termo de referência devem estar disponíveis quando a conexão segura for estabelecida usando:

a. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS;

b. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS;

c. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea.

3.2.37. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deve ser capaz de:

a. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;

b. Encaminhar ao servidor real via cabeçalho HTTP campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS.

3.2.38. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;

3.2.39. Deve possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no appliance e as requisições POP3S, IMAPS e SMTPS são enviadas aos servidores sem criptografia;

3.2.40. A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:

a. SSL session cache Timeout;

b. Session Ticket;

c. OCSP (Online Certificate Status Protocol) Stapling;

d. ALPN (Application Layer Protocol Negotiation);

e. Perfect Forward Secrecy;

3.2.41. Deve possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

3.2.42. Deve ser possível garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;

3.2.43. Deve possuir suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

3.2.44. A solução deve suportar Internet Content Adaptation Protocol (ICAP);

3.2.45. Deve ser capaz de realizar DHCP relay;

3.2.46. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:

a. Tempo de resposta da aplicação;

b. Latência;

c. Conexões para conjunto de servidores, servidores individuais;

d. Por URL.

3.2.47. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:

a. Servidores virtuais;

b. Servidores balanceados;

c. URLs;

d. Países de origem, baseados em geolocalização (GEOIP);

e. Dispositivos de origem do cliente (user agent).

3.2.48. Deve possuir framework unificado para configuração da aplicação;

3.2.49. Deve possuir criptografia para comunicação entre os balanceadores, preferencialmente IPSEC

3.2.50. A solução deve ter a capacidade de realizar cache transparente das respostas DNS;

3.2.51. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;

3.2.52. Deve ter suporte a Transport Layer Security (TLS), Server Name Indication (SNI);

3.2.53. A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;

3.2.54. A solução deve ter suporte a TLS 1.2 e 1.3;

3.2.55. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.

3.2.56. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores;

3.2.57. Deve permitir QoS (Quality of Service) a nível de aplicação ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação;

a. Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes.

3.2.58. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações;

3.2.59. A solução deve permitir a criação de túneis IP transparentes utilizando GRE e IPIP;

3.2.60. Deve possuir suporte ao protocolo SPDY e HTTP 2.0;

3.2.61. A solução deve permitir a sincronização das configurações:

a. De forma automática;

b. Manualmente, forçando a sincronização apenas no momento desejado.

3.2.62. Deve permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

a. Compartilhar a rede de heartbeat com a rede de dados, sendo possível utilizar qualquer endereço IP da RFC 1918;

b. Utilizar uma rede exclusiva para o heartbeat.

3.2.63. Deve permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores: GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version.

3.2.64. Deve ser possível tomar as seguintes ações através dessas políticas:

a. Bloqueio de tráfego

b. Reescrita e manipulação de URL;

c. Registro de tráfego (log);

d. Adição de informação no cabeçalho HTTP;

e. Redirecionamento do tráfego para um membro específico;

f. Selecionar uma política específica para Aplicação Web.

3.2.65. A solução deve ser capaz de fazer log de todas as sessões, no qual os registros deverão conter pelo menos:

a. Endereço IP de origem;

b. Porta de origem;

c. Endereço IP de destino;

d. Porta de destino;

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

f. Data e hora da mensagem;

g. URL acessada;

3.2.66. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory;

3.2.67. A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.

3.3. DNS

3.3.1. A solução deve operar, no mínimo, nas seguintes formas:

a. DNS autoritativo;

b. DNS resolver;

c. DNS cache;

d. Balanceamento de DNS servers;

e. DNSSec.

f. DNS Recursivo;

3.3.2. A solução deve possuir proteções contra ataques DNS, no mínimo:

a. Pacotes malformados;

b. Ataque Teardrop;

c. Ataque ICMP.

3.3.3. A solução deve ser capaz de realizar balanceamento dos servidores DNS;

3.3.4. A solução deve ser capaz de realizar filtragem de pacotes;

3.3.5. A solução deve prover segurança do protocolo DNS, protegendo contra ataques de negação de serviço, NXDOMAIN e reflexão e amplificação de DNS.

3.3.6. A solução deve realizar filtragem de pacotes, preferencialmente stateful inspection;

3.3.7. A solução deve suportar base de Geolocalização IP;

3.3.8. A solução deve implementar DNS64;

3.3.9. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, MX, PTR, SRV e TXT;

3.3.10. Deve ser capaz de gerar estatísticas de DNS;

3.3.11. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;

3.3.12. A solução deve ser capaz de realizar IP Anycast;

3.3.13. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso;

3.3.14. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;

3.3.15. A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;

3.3.16. A solução deve aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;

3.3.17. Deve ser possível ajustar quantos endereços são enviados em uma única resposta;

3.3.18. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido;

3.3.19. Deve suportar pelo menos os seguintes algoritmos de balanceamento:

a. Round Robin;

b. Geografia;

c. Capacidade do Virtual Server;

d. Least Connections;

e. Pacotes por segundo;

f. Round trip time;

g. Hops;

h. Kilobytes per Second;

3.3.20. Deve ser possível implementar persistência da conexão do usuário entre aplicações ou data centers;

3.3.21. A solução deve suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;

3.3.22. A solução deve permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada;

3.3.23. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);

3.3.24. Deve possuir suporte a IPv6 no balanceamento global entre datacenters;

3.3.25. Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6;

3.3.26. Deve possuir a funcionalidade de resposta rápida a queries DNS. Permitindo respostas mais rápidas para zonas que seja autoritativo;

3.3.27. A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes (GSLB) ou encaminhar requisições de clientes (screening);

3.3.28. Baseado no ECS DNS deve ser possível preservar o endereço IP da subnet do cliente ao invés do LDNS para tomar decisões;

3.3.29. A solução deve funcionar pelo menos das seguintes formas:

a. Usar o ECS para tomar decisões de GSLB baseado em topologia (Subnets);

b. Injetar o ECS (proxy requests) para outros servidores DNS.

3.3.30. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver (suporte ECS), o GSLB deve usar a persistência existente para manter o cliente no mesmo Datacenter;

3.3.31. O serviço deve ter a habilidade de detectar, monitorar, controlar e mitigar ataques baseados em DNS sem gerar nenhum impacto ao tráfego válido de DNS;

3.3.32. A solução deve ter serviço de resolução de nomes destinado a armazenar, de forma “autoritativa”, as zonas do CONTRATANTE e o IP reverso do bloco CIDR do CONTRATANTE;

3.3.33. A solução deve ser configurada de forma redundante, permitindo o failover completo na ocorrência de falhas, suportando, no mínimo, o modo de operação ativo-ativo. Um nó deverá suportar sozinho todos os requisitos de performance solicitados neste projeto;

3.3.34. O serviço deve possuir capacidade para resolver consultas para as quais não tem autoridade (ou seja, da zona “.”, tipo “hint”), com a finalidade de atender somente às consultas DNS oriundas da rede interna do CONTRATANTE, bem como dos demais Serviços Gerenciados de Segurança e servidores instalados no Datacenter;

3.3.35. O serviço deve ter, pelo menos, as seguintes características de segurança:

a. Deve permitir o uso de lista negra para bloquear domínios DNS;

b. Deve possuir capacidade de criação de ACLs para bloqueio de domínios e redes maliciosas;

c. Prover uma linha de defesa para bloquear tentativas de acesso a sites maliciosos impedindo a resolução de nomes de domínio que hospedem tais conteúdos maliciosos minimizando possíveis infecções de Malware, Trojan, Spyware, Ransomware e softwares de comando e controle (BotNet);

d. Registrar todas as tentativas de comunicação com os nomes de domínio que hospedem conteúdo malicioso. Estes registros devem conter pelo menos: IP de origem, destino, data e hora do acesso;

3.3.36. Deve suportar no mínimo os seguintes métodos de controle: apenas logar, bloquear o dado ou substituir o nome do domínio;

3.3.37. A solução deve suportar mecanismo de “assinaturas”, ou técnicas semelhantes, que permitam ao fabricante disponibilizar regras de bloqueios contra novos ataques conforme surgimento;

3.3.38. O serviço deve permitir que o administrador crie regras customizadas de bloqueio, da seguinte maneira:

a. Bloqueio de nomes de domínio totalmente qualificados em consultas de DNS feitas via TCP ou UDP.

b. Bloqueio de endereços de origem IPv4 ou IPv6 em consultas realizadas via TCP ou UDP. Esta regra deverá permitir a configuração de endereços de hosts ou de redes;

c. Configuração de limites de quantidades de consultas de DNS (rate limit) realizadas via TCP ou UDP por nome de domínio totalmente qualificado;

d. De acordo com o IP de origem, configurar limite (rate limit) para consultas realizadas via TCP ou UDP;

e. Criar “Listas brancas” que permitam a realização de qualquer número de consultas de DNS por segundo, para determinado endereço IP de origem;

3.3.39. O serviço deverá proteger contra os seguintes ataques de DNS:

a. Negação de Serviço;

b. Negação de Serviços Distribuídos;

c. Amplificação;

d. Explorações (Exploit);

e. Envenenamento do cache;

f. Excessos (Floods).

3.3.40. A administração do serviço deve permitir definir diferentes níveis de grupos e usuários para administração;

3.3.41. O serviço deve possuir capacidade de reverter configurações sem a necessidade de restauração de backup;

3.3.42. O serviço deverá fornecer, no mínimo, os seguintes relatórios:

a. Tendência de latência de resposta de DNS;

b. Tendência de uso do cache de DNS;

c. Top DNS NXDOMAIN/No error;

d. Top SERVFAIL enviados e recebidos;

3.3.43. Deve permitir a criação visões (“views”) para tratamento diferenciado de consultas conforme origem das requisições;

3.3.44. Deve implementar DNSSEC com suporte a NSEC3.

3.4. Firewall

3.4.1. A solução deve atuar preferencialmente como stateful firewall;

3.4.2. A solução deve atuar como full-proxy;

3.4.3. A solução deve terminar as conexões SSL com a finalidade de inspecioná-las;

3.4.4. A solução deve proteger de ataques DDoS nas camadas de rede e de sessão;

3.4.5. A solução deve proteger de ataques DDoS que utilizem SSL;

3.4.6. A solução deve permitir a criação de regras com, no mínimo, os seguintes parâmetros:

a. Endereço IP destino;

b. Endereço IP de origem;

c. Porta de destino;

d. Porta de origem;

e. VLAN;

f. Protocolo.

3.4.7. A solução deve permitir definir agendamento para ativação da regra;

3.4.8. A solução deve permitir definir, no mínimo, as seguintes ações no tráfego:

a. Permitir: os pacotes são aceitos e passam pelo firewall;

b. Rejeitar: os pacotes são rejeitados e ocorre envio de pacotes de destino inatingível ou similar a origem do tráfego;

c. Descartar: onde os pacotes são descartados sem o envio de qualquer notificação a origem do tráfego.

3.4.9. Deve ser possível criar regras que sejam aplicadas em diferentes pontos, no mínimo:

a. Global;

b. Virtual Server.

3.4.10. Deve permitir a configuração de múltiplas contas de usuário local;

3.4.11. Deve fornecer controles de acesso por nível, os quais podem ser atribuídos a usuários ou grupos de usuários para fazer cumprir a separação por perfil de privilégios;

3.4.12. Deve permitir a configuração de alertas que informem automaticamente sobre ataques e anomalia de tráfego, através de thresholds baseados na baseline da rede ou através de limites de tráfego atingido;

3.4.13. Deve permitir a restauração das configurações de proteções originais;

3.4.14. Deve permitir a configuração em alta disponibilidade;

3.4.15. Deve ser possível implementar solução de redundância dos appliances de maneira que em caso de falha de um dos appliances, o outro seja capaz de atender a todas as conexões sem downtime e queda de sessões;

3.4.16. Deve permitir criar lista de exceção de regras (whitelist/blacklist) por endereço IP específico ou faixa de sub-rede;

3.4.17. Deve ser possível bloquear de ataques em serviços HTTP;

3.4.18. Deve ser possível o descarte de sessões TCP ociosas se o cliente não enviar uma quantidade de dados dentro de um período de tempo configurável;

3.4.19. Deve ser possível o bloqueio de requisições DNS na porta 53 malformadas;

3.4.20. Deve ser possível limitar o número de consultas DNS por segundo através da configuração de uma taxa (thresholds);

3.4.21. Deve detectar e descartar pacotes HTTP que não atendam aos padrões RFC e, em seguida, barrar os hosts de origem;

3.4.22. Deve ser possível executar a atualizações necessárias para prevenção de novos ataques;

3.4.23. Deve mitigar, no mínimo, os seguintes tipos de ataques:

a. ICMP/UDP/TCP FloodS;

b. GET/POST FloodS;

c. SYN Floods;

d. Slowloris;

e. Connection Attacks;

f. Botnet.

3.4.24. A solução deve possuir funcionalidade para aumentar o nível de segurança contra ataques DDoS, incluindo a possibilidade de interação com base de reputação de endereços IP e estatísticas de tráfego;

3.4.25. A solução deve possuir relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DoS;

3.4.26. Deve possuir suporte ao envio de SNMP traps para cada ataque DoS detectado;

3.4.27. Deve possuir a funcionalidade de threshold para vetores de DoS. Essa funcionalidade deve valer tanto para proteção do appliance como também para proteção de serviços específicos;

3.4.28. Deve ser possível configurar o sistema para detectar e mitigar assinaturas dinâmicas. Quando configurado, o sistema irá detectar possíveis ameaças DoS baseado no histórico do tráfego e poderá automaticamente mitigar essas ameaças.

3.5. Web Application Firewall

3.5.1. A solução deve operar nos modos ativo-ativo e ativo-passivo;

3.5.2. A solução oferecida deve proteger a infraestrutura web de ataques contra a camada de aplicação (Camada 7);

3.5.3. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado;

3.5.4. A solução deve possuir a capacidade capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador;

3.5.5. A solução deve suportar o uso de firewall camada 3-4 junto com firewall camada 7 no mesmo appliance para evitar problemas com o aumento da latência;

3.5.6. Deve permitir a utilização de um modelo positivo de segurança para proteger contra ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes;

3.5.7. Deve possuir política de segurança de aplicações web pré-configurada na solução;

3.5.8. Deve permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

3.5.9. Deve permitir a criação de políticas diferenciadas por aplicação;

3.5.10. Deve ser possível configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

3.5.11. A solução de WAF deve proteger contra ataques emergentes de camada 7 como SSRF (Server Side RequestForgery);

3.5.12. A solução deve se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas da solução;

3.5.13. A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como por exemplo: Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys e HP Webinspect;

3.5.14. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;

3.5.15. Essa inspeção pode ser feita via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus;

3.5.16. Deve permitir que regras customizadas possam ser utilizadas para customizar e aumentar a proteção contra ataques recentes;

3.5.17. Deve permitir a integração com Firewall de Database de outros fabricantes.

3.5.18. O fabricante da solução deve disponibilizar também a comercialização como serviço na nuvem (WAFaaS) ou estar disponível para contratação em nuvens públicas;

3.5.19. A solução deve permitir incluir em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Portanto o sistema não precisa usar recursos para mitigar tráfego enviado por esses endereços IPs. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de tempo;

3.5.20. A solução deve possuir funcionalidade de proteção positiva e segura contra ataques, como:

a. Acesso por Força Bruta;

b. Ameaças Web AJAX/JSON;

c. DoS e DDoS camada 7;

d. Buffer Overflow;

e. Cross Site Request Forgery (CSRF);
f. Cross-Site Scripting (XSS);
g. SQL Injection;
h. Parameter tampering
i. Cookie poisoning;
j. HTTP Request Smuggling;
k. Manipulação de campos escondidos;
l. Manipulação de cookies;
m. Roubo de sessão através de manipulação de cookies;
n. Força bruta no browser;
o. Checagem de consistência de formulários;
p. Checagem do cabeçalho do “user-agent” para identificar clientes inválidos.

3.5.21. Deve ser capaz de identificar e bloquear ataques através de:
a. Assinaturas, com atualização periódica da base pelo fabricante. As assinaturas devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo a mais por parte da CONTRATANTE na aquisição de novas licenças ou subscrições. Deve fazer parte da solução de WAF ofertada;

3.5.22. Regras de verificação personalizadas – política de segurança configurada;

3.5.23. Deve prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários;

3.5.24. Deve ser possível a customização da resposta de bloqueio;

3.5.25. Deve ser possível a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução;

3.5.26. Deve ser possível limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual;

3.5.27. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração;

3.5.28. Deve permitir criar lista de exceção (whitelist) por endereço IP específico ou faixa de sub-rede;

3.5.29. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10;

3.5.30. Deve ser possível o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

3.5.31. Deverá implantar, no mínimo, as seguintes funcionalidades:

a. Proteção contra Buffer Overflow;
b. Checagem de URL;
c. Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);
d. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);
e. Proteção contra Cross-site Scripting;
f. Funcionalidade de Cookie Encryption;
g. Checagem de consistência de formulários;
h. Checagem do cabeçalho “user-agent” para identificar clientes inválidos.

3.5.32. Deve permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios;

3.5.33. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF);

3.5.34. Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado(s) País/Países seja(m) bloqueado(s);

3.5.35. Deve possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres), cookies, arquivos XML e elementos XML;

3.5.36. A solução oferecida deve possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

3.5.37. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

3.5.38. A solução deve possuir proteção baseada em assinaturas para prover proteção contra ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção à regra geral;

3.5.39. A solução deve permitir o bloqueio de ataques DoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

3.5.40. A solução deve possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:

a. Número de requisições por segundo enviados a uma URL específica;
b. Número de requisições por segundo enviados de um IP específico;
c. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);
d. Número máximo de transações por segundo (TPS) de um determinado IP.

3.5.41. A solução oferecida deve permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;

3.5.42. A solução oferecida deve permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão;

3.5.43. A solução oferecida deverá permitir o cadastro de robôs que possam acessar a aplicação;

3.5.44. A solução oferecido deve implementar proteção ao JSON (JavaScript Object Notation);

3.5.45. Implementar a segurança de web services, através do seguinte método:

3.5.46. Verificação de partes das mensagens SOAP;

3.5.47. Deve prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais;

3.5.48. Deve prevenir que erros de aplicação ou infraestrutura sejam mostrados ao usuário;

3.5.49. Deve ter integração, via ICAP, com servidor de antivírus para verificação dos arquivos a serem carregados nos servidores;

3.5.50. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

3.5.51. Deve armazenar os logs localmente ou exportar para Syslog server;

3.5.52. Deve proteger contra atraques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas;

3.5.53. Deve possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal;

3.5.54. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados: Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade e conformidade com o PCI;

3.5.55. Deve permitir o agendamento de relatórios a serem entregues por email;

3.5.56. Fornecer gráficos de alertas por:

a. Política de segurança;

b. Tipos de ataques;

c. Violações;

d. URL;

e. Endereços IP;

a. Países;

b. Severidade;

c. Código de resposta;

d. Métodos;

e. Protocolos;

f. Usuário;

g. Sessão.

3.5.57. Deverá exportar as requisições que contenham os ataques, pelo menos no formato PDF;

3.5.58. Deve possuir relatório em tempo real sobre ataques DoS L7, atualizado automaticamente;

3.5.59. Possuir método de mitigação de DoS L7 baseado em:

a. Descarte de todas as requisições de um determinado IP e/ou país suspeito;

b. Geolocalização;

c. Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô;

3.5.60. A solução deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente;

3.5.61. A solução deve classificar o nível de violação de uma requisição, possuindo pelo menos 5 níveis, onde o nível 5 é referente à violação mais grave e, portanto, deve ter prioridade.

3.5.62. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual;

3.5.63. Suportar codificação HTML "application/x-www-form-urlencoded";

3.5.64. Suportar Criptografia de Cookies;

3.5.65. Suportar codificação fragmentada (chunked encoding) em requisições e respostas;

3.5.66. Suportar compressão de requisições e respostas;

3.5.67. Suportar validação de protocolo, como:

a. Possibilidade de restringir uso de métodos;

b. Possibilidade de restringir protocolos e versões de protocolos;

c. Strict (per-RFC) Request Validation;

d. Validar caracteres URL-encoded;

e. Validação de codificação fora de padrão %uXXYY.

3.5.68. Suportar restrições de HTML, como:

a. Nome de parâmetros;
b. Tamanho e tipo dos valores de parâmetros;
c. Combinação de nome, tipo e tamanho de parâmetros.

3.5.69. Suportar POST no upload de arquivo;

3.5.70. Permitir configurar ou oferecer restrições para tamanho individual de arquivo;

3.5.71. Suporte para os métodos Basic, Digest e NTLM para autenticação;

3.5.72. Capacidade de filtrar cabeçalhos, corpo e status de respostas;

3.5.73. Suportar as seguintes técnicas de detecção:

a. URL-decoding;
b. Case de caracteres misturados;
c. Uso excessivo de espaços em branco;
d. Remoção de comentários;
e. Caracteres de escape.

8.1.2. Deve possuir registro de logs com as seguintes características:

a. Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;
b. Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que permita a exportação ou em outro formato aberto como CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de dados;
c. Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log.

3.5.74. A solução deve permitir gerar relatórios em formatos PDF e HTML.

3.5.75. Possuir as seguintes características de gerenciamento:

a. Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de falso positivo;
b. Facilidade para transformar um ataque detectado e considerado falso positivo como regra do firewall;
c. Facilidade para aplicar diferentes regras para diversas aplicações;
d. Capacidade para customizar regras de negação de serviço;
e. Capacidade para combinar detecção e prevenção na construção das regras;
f. Capacidade para desfazer a aplicação de uma regra.

3.5.76. A solução deve apresentar perfil de aprendizagem automática com:

a. Capacidade de aprendizagem automática sem intervenção humana;

b. Capacidade de inspeção das regras criadas automaticamente.

3.5.77. Deve ser possível o gerenciamento da configuração com as seguintes características:

a. Gerenciamento por autenticação dos usuários e as autorizações baseadas em perfis (roles);

b. Capacidade de gerenciamento remoto da solução.

3.5.78. Deve ser possível apresentar logs e relatórios administrativos com as seguintes características:

a. Capacidade para identificar e notificar falhas do sistema ou perda de performance;

b. Capacidade de agregação de informações para simplificar a revisão das atividades do dispositivo;

c. Capacidade para gerar estatísticas de serviço e sistema.

3.5.79. Deve possuir suporte a XML:

a. Para proteção de WebServices;

b. Em conformidade com a especificação WS-I básico;

c. Com capacidade de restringir métodos do WebService via definição em WSDL.

3.5.80. Com capacidade de realizar filtro e validação de funções XML específicas de uma aplicação.

3.5.81. Deve suportar funções de camuflagem (cloaking), como:

a. Esconder qualquer mensagem de erro http dos usuários;

b. Remover as mensagens de erro das páginas que serão enviadas aos usuários.

3.5.82. Deve ser possível proteger a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e técnicas avançadas de análise comportamental;

3.5.83. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS;

3.5.84. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;

3.5.85. Deve possuir uma proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque;

3.5.86. Deve possuir proteção contra ataques DDoS, através da análise de comportamento de trafego usando técnicas de análise de dados e Machine Learning;

3.5.87. Através da análise contínua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitigá-las;

3.5.88. Deve ajudar a prevenir contra ataques de Credential Stuffing, onde bases de credenciais expostas na Internet são usados para tentativa de acesso de outras aplicações Web;

3.5.89. Implementar políticas de WAF em aplicações HTTP/1, HTTP/1.1 e HTTP/2;

3.6. Identificação e Acesso

3.6.1. Deverá implementar as funcionalidades de Single Sign-on e VPN-SSL, com os seguintes recursos:

a. Deve possuir o modo “Portal” onde a solução se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;

b. Deve possuir o modo “Network”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna.

3.6.2. Deve possuir suporte a split tunneling;

3.6.3. Deve possuir suporte à compressão HTTP;

3.6.4. Deve permitir estabelecimento de conexão segura de acesso remoto sem a necessidade de instalação de um software cliente na máquina do usuário;

3.6.5. Deve possibilitar a customização da interface gráfica da página de Login e mensagens de apresentação ao usuário;

3.6.6. Deve oferecer acesso remoto seguro à rede inteira para qualquer aplicação baseada em IP (TCP ou UDP);

3.6.7. Deverá possuir ativo o controle de, no mínimo, 3000 usuários concorrentes, e deverá vir com todo o licenciamento necessário para ativação do número de usuários solicitados;

3.6.8. Deve ter suporte a Single-Sign-On (SSO), com os seguintes recursos:

a. Deverá ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação;

b. Deve ser capaz de realizar single-sign-on utilizando kerberos;

c. Deve ser capaz de fazer cache das credenciais do usuário e utilizar a credencial correta para cada sistema;

d. Deve ser capaz de implementar SSO mesmo quando conectado via modo “Network”, quando o usuário chama o portal digitando o site diretamente no browser (sem clicar pelo portal).

3.6.9. Deverá implementar suporte à validação da estação do usuário para, no mínimo, os seguintes recursos:

a. Versão do Sistema Operacional;

a. Firewall ativado;

b. Antivírus instalado;

c. Antivírus atualizado;

d. Processos em execução;

e. Certificados digitais instalados na máquina.

f. Deverá ser possível configurar uma ação dependendo da validação da estação do usuário;

3.6.10. Deverá permitir conferência do endereço IP quanto à origem Geográfica, permitindo a criação de regras de acesso de acordo com o país ou estado de origem. A base de dados de endereços IP deverá estar presente na solução, e deverá ser atualizada periodicamente pelo fabricante da solução sem custo adicional;

3.6.11. Deve suportar autenticação de múltiplos fatores utilizando tokens de hardware e software;

3.6.12. Deverá ser capaz de autenticar usuários em bases de dados LDAP, RADIUS, TACACS+, ou Active Diretor;

3.6.13. Deve possuir capacidade para definir diversos métodos para acesso remoto;

3.6.14. Deve possuir capacidade para suportar múltiplos navegadores;

3.6.15. Deve possuir capacidade para definir autenticação e autorização web dos usuários para acesso ao virtual server (access sessions);

3.6.16. Deve possuir capacidade para definir perfil de acesso a rede através de wizard;

3.6.17. Deve possuir capacidade para definir o tempo de inatividade antes de encerrar a sessão do usuário;

3.6.18. Deve possuir capacidade para definir o tempo máximo de conexão para sessão do usuário;

3.6.19. Deve possuir capacidade para definir a quantidade máxima de usuários por servidor virtual;

3.6.20. Deve possuir capacidade para definir a quantidade máxima de sessões por usuário;

3.6.21. Deve possuir capacidade para definir os recursos de DNS;

3.6.22. Deve possuir capacidade para definir os recursos de AAA;

3.6.23. Deve possuir capacidade para realizar múltiplos métodos de autenticação remotos: RADIUS, LDAP, ACTIVE DIRECTORY, HTTP, TACACS+, KERBEROS;

3.6.24. Deve possuir capacidade para finalizar a sessão do usuário com base em número X de tentativas com erro;

3.6.25. Deve possuir capacidade para permitir a troca da senha dos usuários que tenham expirado;

3.6.26. Deve possuir capacidade para definir lease pool que contenha endereços IP a serem designados aos usuários com acesso à rede (endereço do cliente PPP);

3.6.27. Deve possuir capacidade para definir servidor virtual em HTTPS com perfil cliente SSL padrão;

3.6.28. Deve possuir capacidade de redirecionar tráfego HTTP para HTTPs para um determinado servidor virtual;

3.6.29. Deve possuir capacidade para definir que todo tráfego seja tunelado;

3.6.30. Deve possuir capacidade para definir perfil de acesso ao portal através do wizard;

3.6.31. Deve possuir capacidade para realizar proxy reverso com a finalidade de "ofuscar" a URI promovendo assim o acesso seguro as aplicações web internas;

3.6.32. Deve possuir capacidade para personalizar as páginas de login/logout para determinados usuários e grupos de usuários;

3.6.33. Deve possuir capacidade para realizar Single Sign On (SSO): NTLM v1 & v2, BASIC, HTTP FORMS BASED, KERBEROS;

3.6.34. Deve possuir capacidade para personalizar a página de SSO;

3.6.35. Deve possuir capacidade para exibir múltiplas páginas de SSO baseadas em recursos individuais ou de grupo;

3.6.36. Deve possuir capacidade para descobrir dentro do web browser do usuário qual idioma designado;

3.6.37. Deve possuir capacidade para realizar verificações e validações no dispositivo do cliente antes de conceder acesso: ANTI-VIRUS, FIREWALL, FILE/PROCESS, REGISTRY ENTRY, MACHINE CERTIFICATE;

3.6.38. Deve possuir capacidade para realizar verificações e validações no servidor antes de conceder acesso: OS DETECTION, GEOLOCATION IP, CLIENT APPLICATION;

3.6.39. Deve possuir capacidade para conceder acesso a usuários autorizados os recursos específicos ou grupo de recursos;

3.6.40. Deve possuir capacidade para definir bookmark para páginas web externas;

3.6.41. Deve possuir capacidade para utilizar compressão nas aplicações pré-determinadas;

3.6.42. Deve possuir capacidade para atribuir a qualquer aplicação com front-end web autenticação e autorização de usuários sem alteração do código da aplicação;

3.6.43. Deve possuir capacidade para definir web perfil de acesso a aplicação através de wizard;

3.6.44. Deve prover acesso remoto através de VPN SSL para Microsoft Windows, Linux, dispositivos baseados em Android e iOS e MAC OSX;

3.6.45. Suportar autenticação de usuários em AAA;

3.6.46. O sistema deve inspecionar se no cliente existe antivírus e firewall instalados antes de prover o acesso remoto. Essa verificação deverá ocorrer em sistemas operacionais de desktops;

3.6.47. Com base na análise do cliente, o sistema deverá conceder dinamicamente o acesso ao usuário: se o cliente estiver adequado com as políticas de segurança poderá acessar os recursos definidos em sua autenticação, caso contrário deverá ter acesso limitado definidos pelo administrador;

3.6.48. Deve suportar acesso a serviços de terminais através de:

a. Citrix XenApp;

b. Citrix XenDesktop;

c. Microsoft RDP;

d. VMware Horizon View.

3.6.49. A solução deve realizar federação através de SAML Artifact Binding onde a comunicação será direta entre o Identity Provider (IdP) e o Service Provider (SP);

3.6.50. A solução deverá atuar como gateway para o acesso MSRDP, deverá ser possível realizar autenticação via NTLM dos usuários, sem a necessidade de software adicional;

3.6.51. A Solução deve permitir o uso de one-time passcode (OTP) como segundo fator de autenticação.

3.7. Inspeção SSL

3.7.1. A solução deve suportar o método de implementação em alta disponibilidade com dois appliances para manter o serviço operacional. Deve ainda possuir resiliência de sessão TCP entre os appliances;

3.7.2. A solução deve prover visibilidade SSL/TLS tanto para o tráfego de entrada (Datacenter) quanto para o tráfego de saída (usuários), permitindo que uma solução em appliance centralizada seja responsável por orquestrar e distribuir dinamicamente o tráfego entre os dispositivos de segurança na camada de inspeção;

3.7.3. A solução deve tomar decisões inteligentes de acordo com o contexto de tráfego, enviando somente a cadeia de dispositivos de segurança que precisam visualizar esse contexto de tráfego;

3.7.4. A solução deve, portanto, evitar a topologia tradicional de "ligação em cascata" dos dispositivos de segurança, em que o tráfego precisa necessariamente passar por todos os dispositivos de segurança sempre;

3.7.5. A solução deve trabalhar com direcionamento de tráfego inteligente e dinâmico baseado em políticas de contexto, permitindo o gerenciamento de fluxo inteligente entre os dispositivos de segurança e garantindo a disponibilidade de acesso;

3.7.6. A solução deve usar os dispositivos de segurança com maior eficiência através da política de contextualização de tráfego;

3.7.7. Deve monitorar cada dispositivo de segurança independentemente, permitindo realizar o bypass ou não caso o mesmo esteja com problemas;

3.7.8. Deve permitir a escalabilidade independente de cada dispositivo de segurança. Portanto, se for necessário inserir por exemplo mais um dispositivo IPS na zona de inspeção, a solução deve ser configurada para distribuir o tráfego entre os dispositivos IPS ativos;

3.7.9. Deve permitir escalar os dispositivos de segurança com alta disponibilidade, usando probes de monitoração de saúde para identificar o estado de cada solução de segurança;

3.7.10. A solução deve permitir que múltiplos equipamentos de segurança de diversos fabricantes tenham visibilidade tanto do tráfego de saída quanto entrada, fazendo que os mesmos continuem realizando suas inspeções procurando por malwares e exfiltração de dados;

3.7.11. A solução deve possuir suporte a diversas cifras e protocolos SSL/TLS;

3.7.12. A solução deve fazer a monitoração dos serviços dentro da camada de inspeção;

3.7.13. A solução deve permitir a resiliência dos serviços dentro da zona de inspeção, inclusive fazendo o balanceamento de carga entre múltiplos equipamentos do mesmo serviço;

3.7.14. A solução deve suportar SSL forward secrecy como uma forma de melhorar a segurança nas transações SSL/TLS;

3.7.15. A solução deve atuar de forma inline, com o tráfego sendo desviado para a mesma;

3.7.16. Deve implementar SSL offload, ou seja, realizar a encriptação e decriptação das sessões SSL;

3.7.17. Deve suportar modo Explicit Proxy;

3.7.18. Deve suportar modo Transparent Proxy;

3.7.19. Deve dar a opção de ações caso o certificado original do servidor expire;

3.7.20. Deve dar a opção de fazer o bypass do tráfego caso falhe o TLS handshake;

3.7.21. Deve suportar implantação em linha em Layer 2;

3.7.22. Deve suportar implantação em linha em Layer 3;

3.7.23. Deve suportar o envio de tráfego para dispositivos em linha em Layer 2 e 3, conectando-se diretamente ao dispositivo de descriptografia e também através de um switch, desacoplando o dispositivo de segurança da interface física, porta ou VLAN;

3.7.24. Deve suportar o envio de tráfego ICAP para dispositivos;

3.7.25. Deve ser capaz de enviar tráfego para dispositivos passivos, como DLPs;

3.7.26. Deve ser capaz de balancear tráfego entre dispositivos de inspeção;

3.7.27. Deve ser capaz de enviar o tráfego original para dispositivos de inspeção;

3.7.28. Deve ser capaz de monitorar a integridade de dispositivos por meio de sondagem (probes);

3.7.29. Deve ser capaz de fazer direcionamento do tráfego descriptografado baseado em políticas;

3.7.30. Deve ser capaz de criar múltiplos Service Chains;

3.7.31. Deve ser capaz de fazer bypass da inspeção com base em categoria ou URL;

3.7.32. Deve implementar a renegociação de sessão;

3.7.33. Deve implementar geração de chaves RSA, enrollment de certificado, importação e exportação de chaves, certificados de servidores;

3.7.34. Deve implementar autenticação, autorização e registro das operações dos administradores através dos protocolos TACACS+ e RADIUS;

3.7.35. Deve possuir MIB SNMP;

3.7.36. Deve possuir redundância ativo/standby com sincronismo dos estados das conexões dos usuários assim como suas características de atribuição de servidores;

3.7.37. Deve permitir que ferramentas de segurança recebam o tráfego descriptografado da solução e tomem decisões para mitigar ataques, incluindo firewalls em camada 2 e 3, IPS e web proxies;

3.7.38. Deve otimizar a infraestrutura SSL, provendo visibilidade para variadas soluções de segurança sobre o tráfego SSL/TLS;

3.7.39. Deve suportar fazer “traffic steering” para as soluções de segurança;

3.7.40. Deve possuir inteligência baseada em contextos para tratar o tráfego criptografado;

3.7.41. Deve centralizar as operações de criptografia/descriptografia, provendo a mais moderna tecnologia de encriptação SSL com grande variedade de cifras e protocolos;

3.7.42. Deve permitir maior flexibilidade e escalabilidade de diferentes soluções de segurança;

3.7.43. Deve ser possível distribuir carga, utilizando técnicas de balanceamento para as soluções de segurança como por exemplo Firewalls;

3.7.44. Deve realizar checagem de saúde para identificar se as soluções de segurança estão funcionando sem problemas. Caso haja alguma falha em determinada solução deve ser possível fazer o by-pass e não passar o tráfego para essa solução, não prejudicando o acesso do cliente;

3.7.45. Deve ser possível reduzir o custo administrativo com o uso de políticas inteligentes baseado em contextos, permitindo maior eficiência no envio de tráfego para as soluções relevantes e maior efetividade no uso dos diversos equipamentos de segurança;

3.7.46. Deve possuir um controle granular sobre mudanças no cabeçalho HTTP e suporte a traduções de porta que permitem aos dispositivos de segurança identificarem um tráfego em texto claro (ex: HTTP) para a devida inspeção;

3.7.47. Através de políticas baseadas em contextos, deve ser possível reduzir custos administrativos, removendo o gerenciamento de chaves e certificados dos equipamentos de segurança;

3.7.48. Deve ser possível ainda reduzir a latência de inspeção SSL atual que é realizada em diversos equipamentos de segurança, centralizando essa operação de criptografia/descriptografia num dispositivo único;

3.7.49. Deve permitir enviar o tráfego descriptografado para análise de diversos equipamentos de segurança como por exemplo: Firewalls, Proxy Web, DLP, anti-malware, IPSs, ferramentas forenses, etc;

3.7.50. Deve suportar fazer o offload da autenticação na solução de visibilidade SSL e passar de alguma forma esse usuário autenticado para o serviço de Web proxy;

3.7.51. Deve suportar equipamentos de segurança de diversos fabricantes;

3.7.52. Deve suportar uma grande diversidade de cifras SSL;

3.7.53. Deve ser possível melhorar a utilização e disponibilidade dos equipamentos de segurança através de técnicas de balanceamento e monitoração;

3.7.54. Deve realizar descriptografia de SSL/TLS independente da porta TCP;

3.7.55. Deve suportar pelo menos as seguintes cifras e protocolos: TLS1/1.1/1.2, SHA, SHA2, AES-GCM, AES;

3.7.56. Deve suportar ECDHE, RSA e DHE com suporte a Forward Secrecy;

3.7.57. Deve oferecer controle a nível de Proxy nas cifras e protocolos, permitindo uma negociação entre o cliente e a solução e outra negociação entre a solução e o serviço;

3.7.58. Deve permitir ser implementado pelo menos com dispositivos: HTTP Web Proxy, Roteados (L3) e inline (L2), serviços DLP/ICAP e dispositivos que apenas recebem o tráfego como por exemplo IDSs;

3.7.59. A solução deve atuar como um Proxy, negociando as cifras e protocolos tanto com o cliente quanto com o servidor.

ANEXO II Modelos de Documentos

MODELO – PROPOSTA

LOTE 1

AQUISIÇÃO DE SOLUÇÃO DE CONTROLE DE ENTREGA DE APLICAÇÕES (ADC) COM FUNCIONALIDADES DE FIREWALL DE APLICAÇÃO WEB (WAF) E BALANCEAMENTO DE CARGA (LOAD BALANCE) COM SUPORTE TÉCNICO E GARANTIA INCLUSOS NO LICENCIAMENTO PELO PERIODO DE 36 MESES E SERVIÇO DE IMPLANTAÇÃO, CONFORME ESPECIFICAÇÕES ABAIXO E TERMO DE REFERÊNCIA.

ITEM	DESCRIÇÃO	TIPO	QTD	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
01	Licenciamento de Controlador de Entrega de Aplicativos (ADC) virtual (Appliance virtual) com recursos de Firewall de Aplicação Web (WAF) e Balanceamento de carga (Load Balance) com garantia e Suporte Técnico por 36 meses	UN	02		
02	Serviço de implantação da solução (com passagem de conhecimento)	SV	01		
PREÇO GLOBAL PARA O LOTE 01 (R$) – Itens 01 e 02					

Informações do produto

Nome do produto	Modelo (Part Number)	Descrição da garantia do fabricante	Descrição do suporte oferecido pelo fabricante

MODELO – ATENDIMENTO ÀS ESPECIFICAÇÕES TÉCNICAS

Modelo meramente sugestivo. A comprovação de atendimento das especificações técnicas pode ser apresentada por meio de modelo específico do licitante ou utilizando a planilha Excel disponibilizada.

Fornecedor:_____CNPJ:_____

Produto:_____Modelo:_____

Indicador da Exigência Técnica	Documento	Página do respectivo documento

MODELO – TERMO DE RECEBIMENTO DEFINITIVO

Contrato:	
Serviço:	
Fiscal Técnico do contrato:	
Gestor do contrato:	

CRITÉRIO DE CONFERÊNCIA				
ITEM	**ASPECTOS QUANTITATIVOS**	**SIM**	**NÃO**	**N/A**
01	A contratada concluiu a implantação da solução no prazo?	☐	☐	☐
02	A contratada entregou relatório gerencial no prazo?	☐	☐	☐
ASPECTOS QUALITATIVOS				
03	A contratada entregou o Relatório Final de Implantação?	☐	☐	☐
04	Foi disponibilizado pela CONTRATADA as informações e acessos para abertura de chamados de suporte técnico?	☐	☐	☐
05	O produto entregue corresponde ao previsto na proposta da empresa?	☐	☐	☐
06	A CONTRATADA realizou o repasse de conhecimento (hands on) para a equipe técnica do TJMS?	☐	☐	☐
ASPECTOS CONTRATUAIS				
07	As licenças estão registradas no site do fabricante em nome do TJMS?	☐	☐	☐
08	O valor dos produtos descritos na nota fiscal corresponde ao previsto na contratação?	☐	☐	☐
09	O CNPJ constante da nota fiscal corresponde ao expresso no empenho?	☐	☐	☐

RELÁTORIO DE OCORRÊNCIAS

RECEBIMENTO DEFINITIVO DO OBJETO	
Efetuada a análise de conformidade do objeto com as especificações do Termo de Referência e do instrumento contratual, quanto aos aspectos quantitativos, qualitativos e de obrigações contratuais, a fiscalização decide, ressalvadas eventuais observações contidas no Relatório de Ocorrências, por:	
☐	**RECEBER** definitivamente o objeto**.**
☐	**NÃO RECEBER** definitivamente o objeto.

Campo Grande, _____de_____de 2024.

Equipe de fiscalização do Contrato:

Fiscal técnico do contrato	Gestor do Contrato

MODELO DE DECLARAÇÃO DE IMPLANTAÇÃO DE SERVIÇO

Declaração

A [Nome da Empresa] declara formalmente a conclusão da implantação da solução de Controle de Entrega de Aplicações (ADC) [Nome do Produto] para o Tribunal de Justiça do Estado do Mato Grosso do Sul, conforme o contrato [Número do Contrato] e o termo de referência.

Confirmamos que todos os serviços foram implementados em conformidade com os requisitos especificados no termo de referência e estão plenamente operacionais.

Campo Grande, _____de_____de 2024.

_____

Responsável (Nome/Cargo/Assinatura)
Nome da Empresa

MODELO DE RELATÓRIO FINAL DE IMPLANTAÇÃO

Relatório Final de Implantação

Contrato	
Nome da Empresa	
Preposto	
Contato	

- **Introdução:**
  - Breve descrição do projeto e seu escopo.
  - Objetivos da implantação da solução.
- **Metodologia de Implantação:**
  - Descrição das metodologias e processos usados na implantação.
- **Detalhamento das Etapas de Implantação:**
  - Descrição detalhada de cada etapa da implantação, incluindo:
    - Configurações realizadas.
    - Ajustes e customizações.
    - Testes conduzidos e resultados.
- **Conformidade com o Termo de Referência:**
  - Análise detalhada de como cada requisito do termo de referência foi atendido.
- **Resultados dos Testes de Conformidade e Funcionamento:**
  - Detalhamento dos testes realizados (incluindo testes de penetração, se aplicável) e resultados obtidos.
- **Desafios e Soluções:**
  - Descrição dos desafios encontrados durante a implantação e como foram resolvidos.
- **Conclusão:**
  - Avaliação geral do projeto de implantação.
  - Confirmação de que o serviço está operacional e atende aos requisitos estabelecidos.
- **Anexos (se aplicável):**
  - Documentos de suporte, gráficos, tabelas, etc.

Campo Grande, _____de_____de 2024.

_____
Responsável (Nome/Cargo/Assinatura)
Nome da Empresa

ANEXO III – Quadro de prazos

EVENTO	DESCRIÇÃO	PRAZO
01	Assinatura do contrato	Até **05 dias uteis**, a partir da convocação formal pela Coordenadoria de Contratos, Convenio e Afins.
02	Reunião inicial	Em até **15 dias** após assinatura do contrato
03	Início da execução da implantação da solução	Em até **30 dias** após assinatura do contrato
04	Entrega das licenças	Em até **30 dias** após assinatura do contrato
05	Entrega da solução implantada	Em até **60 dias** após assinatura do contrato
06	Passagem de conhecimento	Em até **70 dias** após assinatura do contrato
07	Entrega declaração de implantação e relatório final de implantação	Na data do **Evento 05**
08	Recebimento definitivo	Em até **5 dias** após o **Evento 07**
09	Envio da nota fiscal	Após o **Evento 08**
10	Pagamento	Em até **10 dias** úteis após o **Evento 08**