



JUSTIÇA FEDERAL
CONSELHO DA JUSTIÇA FEDERAL

TERMO DE REFERÊNCIA N. 0735724/CJF

1. Definição do objeto (Art. 6º, XXIII, "a", Lei n. 14.133/2021)

a) Contratação de empresa especializada, por meio de Registro de Preços – SRP, para o fornecimento de solução tecnológica de Controlador de Entrega de Aplicações (*Application Delivery Controller* – ADC), incluindo os serviços de instalação, configuração, suporte técnico mensal e transferência de conhecimento, bem como serviços técnicos especializados, sob demanda, para implementação e customização da solução, conforme especificações técnicas contidas neste Termo de Referência e seus anexos, com vistas a atender às necessidades do Conselho da Justiça Federal e demais órgãos partícipes.

b) O fornecimento dos bens e serviços, descritos neste Termo de Referência, é composto dos seguintes itens:

Grupo	Item	Especificação	Unidade	Qtd. CJF	Qtd. TRF3	Qtd. JFSP	Qtd. JFMS	Qtd. TRF5	Qtd. JFPE	Qtd. JFCE	Qtd. JFPB	Qtd. JFAL	Qtd. JFSE	Qtd. JFRN	Qtd. TRF6
1	1.1	Appliance físico para solução de <i>Application Delivery Controller</i> – ADC, fabricante F5, Modelo BIG-IP R4800	Unidade	2	2	2	2	0	0	0	0	0	0	0	2
	1.2	Serviço de instalação e configuração da solução ADC	Unidade	2	2	2	2	0	0	0	0	0	0	0	2
	1.3	Serviço de garantia e suporte técnico presencial para a solução ADC	Mês	60	60	60	60	0	0	0	0	0	0	0	60
	1.4	Transferência de conhecimento <i>online</i> , com carga horária mínima de 40h	Pessoa	4	10	0	0	0	0	0	0	0	0	0	6
	1.5	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	2400	120	120	120	0	0	0	0	0	0	0	200
2	2.1	Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	0	0	0	0	0	0	0	2	2	2	2	0
	2.2	Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	0	0	0	0	2	2	2	0	0	0	0	0
	2.3	Serviço de instalação e configuração da solução ADC	Unidade	0	0	0	0	2	2	2	2	2	2	2	0
	2.4	Serviço de suporte técnico remoto para a solução ADC	Mês	0	0	0	0	12	12	12	12	12	12	12	0

2.5	Transferência de conhecimento <i>online</i> , com carga horária mínima de 40h	Pessoa	0	0	0	0	3	3	3	3	3	3	3	0
2.6	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	0	0	0	0	200	200	200	200	200	200	200	0

1.1. Compõem este Termo de Referência os seguintes anexos:

- 1.1.1. Anexo I – Detalhamento dos requisitos técnicos do objeto para o Grupo 1;
- 1.1.2. Anexo II – Detalhamento dos requisitos técnicos do objeto para o Grupo 2;
- 1.1.3. Anexo III – Arquitetura Proposta para Instalação da Solução no CJF;
- 1.1.4. Anexo IV – Cronograma de Implantação;
- 1.1.5. Anexo V – Planilha de Composição de Custos;
- 1.1.6. Anexo VI – Termo de Confidencialidade e Sigilo da Contratada;
- 1.1.7. Anexo VII – Termo de Vistoria.

1.2. Requisitos da contratação (Art. 6º, XXIII, "d" c/c art. 18, §1º, III, Lei n. 14.133/2021)

- 1.2.1. Os requisitos técnicos das soluções de *Application Delivery Controller* – ADC, tanto para os *appliances* físicos (GRUPO 1) quanto para os *appliances* virtuais (GRUPO 2), a serem adquiridas por meio da presente contratação, são apresentados nos Anexo I – Detalhamento dos requisitos técnicos do objeto para o Grupo I e Anexo II – Detalhamento dos requisitos técnicos do objeto para o Grupo 2 deste Termo de Referência;
- 1.2.2. Para as condições de execução dos demais serviços a serem prestados pela CONTRATADA durante a vigência contratual, deverá ser observado o item 4 -Modelo de execução e de gestão do contrato deste documento.

1.2.1 Requisitos de negócio

- 1.2.1.1 A solução contratada deverá ser capaz de realizar a aceleração de aplicações, com vistas ao melhoramento do desempenho da aplicação e o tempo de resposta em conexões de rede;
- 1.2.1.2 A solução contratada deverá implementar mecanismos de QoS (*Quality of Service* ou Qualidade de Serviço) de forma a garantir o desempenho e a disponibilidade de aplicações essenciais quando houver limitação dos recursos de rede. Dentre esses mecanismos, devem, minimamente, compor a solução os seguintes:
 - 1.2.1.2.1 Mecanismo de modelagem de tráfego (*traffic shaping*), a qual possibilita o gerenciamento da largura de banda para garantir que as informações relativas às aplicações prioritárias sejam entregues sem atrasos;
 - 1.2.1.2.2 Mecanismo de descarregamento de SSL (*SSL offloading*), o qual consiste no processo de remover a criptografia baseada em SSL (*Secure Socket Layer*) do tráfego de entrada para aliviar os servidores de aplicação da carga de processamento de descryptografia e/ou criptografia;
 - 1.2.1.2.3 Mecanismo de balanceamento de carga (*load balancing*), o qual atua como proxy reverso e distribui o tráfego de rede entre os *endpoints* em vários servidores disponíveis;
 - 1.2.1.2.4 Mecanismo de *caching*, o qual pode armazenar em memória interna conteúdos requisitados com maior frequência pelos usuários, de forma que a resposta para determinadas requisições seja ainda mais rápida.
- 1.1.1.3 A solução contratada deverá implementar o mecanismo de *firewall* de aplicação web (WAF – *Web Application Firewall*) com vistas a proteger as aplicações de diversos ataques da camada de aplicação, como *cross-site scripting* (XSS), injeção de SQL, envenenamento de cookies, entre outros.
- 1.1.1.2.2 Mecanismo de segurança contra ataques do tipo negação de serviço (DoS e DDoS), os quais abusam da largura de banda e sobrecarregam os recursos de rede;
- 1.1.1.4 A solução adquirida deverá possibilitar a interconexão de mais de um *appliance* ADC para a composição de uma rede de controle de entrega de aplicação fisicamente distribuída;

1.1.1.5 A solução adquirida deverá possuir aplicação embarcada que permita acesso via navegador web e que possibilite realizar as configurações e o monitoramento do *appliance*.

1.1.1.6 Para a solução composta por *appliances* físicos, cada unidade de *appliance* deverá ser composta por um único equipamento monolítico, o qual possibilite a instalação física em rack específico para *data center* (padrão 19 polegadas);

1.2.2 Requisitos temporais

1.2.2.1 Todos os requisitos temporais serão aplicados para ambos os tipos de solução, seja ela composta por *appliances* físicos ou virtuais, salvo quando houver diferenciação expressamente escrita;

1.2.2.2 A CONTRATADA deverá entregar todos os equipamentos e componentes (sejam físicos ou virtualizados), bem como os acessórios da solução no prazo máximo de até 45 (quarenta e cinco) dias corridos, a contar da data de emissão da Ordem de Serviço;

1.2.2.3 A CONTRATADA e o CONTRATANTE deverão realizar **em até 5 (cinco) dias corridos**, após a emissão da Ordem de Serviço, a Reunião Inicial de Planejamento, a ser realizada, preferencialmente, no formato presencial, na sede do CONTRATANTE, ou, alternativamente, por meio de videoconferência;

1.2.2.3.1 A CONTRATADA deverá apresentar o seu Preposto, Gerente de Projetos e Responsável Técnico na ocasião da Reunião Inicial de Planejamento;

1.2.2.4 A CONTRATADA deverá apresentar o Plano de Implantação, **em até 10 (dez) dias corridos** contados da realização da Reunião Inicial de Planejamento, contendo a documentação detalhada das atividades de entrega dos equipamentos, instalação da solução tecnológica, configuração e testes dos equipamentos que compõem a solução;

1.2.2.5 A Equipe de Fiscalização do CONTRATANTE fará a emissão do primeiro Termo de Recebimento Provisório (TRP1), referente à etapa da entrega dos equipamentos da solução, **em até 5 (cinco) dias corridos** contados da comunicação da CONTRATADA;

1.2.2.6 A CONTRATADA deverá realizar a instalação e configuração dos appliances que compõem a solução no prazo máximo de 20 (vinte) dias corridos, contados a partir da data de emissão do primeiro Termo de Recebimento Provisório (TRP1);

1.2.2.7 A Equipe de Fiscalização do CONTRATANTE fará a emissão do segundo Termo de Recebimento Provisório (TRP2), referente à etapa de instalação e configuração dos equipamentos da solução, **em até 5 (cinco) dias corridos** contados a partir da comunicação da CONTRATADA;

1.2.2.8 A Equipe de Fiscalização Técnica ou o Gestor do CONTRATANTE fará a emissão do Termo de Recebimento Definitivo (TRD) referente à entrega, instalação, configuração e licenciamento da solução **em até 10 (dez) dias corridos** contados a partir da emissão do segundo Termo de Recebimento Provisório (TRP2);

1.2.2.8.1 Após a emissão do TRD, iniciará o período vigência contratual no qual a CONTRATADA fará jus ao pagamento relativo ao serviço de suporte técnico.

1.2.2.8.2 O dia do mês em que ocorrer a emissão do TRD será o marco inicial para a contagem dos períodos mensais relativos ao serviço de suporte técnico. Assim, cada período mensal se iniciará no dia indicado pela emissão TRD e se estenderá até o dia anterior do mês subsequente. **Exemplo:** se o TRD for emitido no dia 10 (dez) de um certo mês, então cada período mensal se iniciará sempre no dia 10 (dez) de cada mês e se estenderá até o dia 9 (nove) do mês seguinte.

1.2.2.9 Na hipótese de ser verificada a não adequação do objeto nas etapas de entrega ou de implantação e configuração da solução, conforme requisitos técnicos, a Equipe de Fiscalização Técnica ou o Gestor o rejeitará imediatamente, no todo ou em parte, devendo a CONTRATADA proceder à regularização no **prazo máximo de 15 (quinze) dias corridos** após a notificação;

1.2.2.10 O CONTRATANTE poderá emitir Ordem(ns) de Serviço específica(s) para a realização da ação de Transferência de Conhecimento **a partir de 20 (vinte) dias corridos** após a emissão do TRD.

1.2.2.11 Após emissão da Ordem de Serviço específica para a ação de Transferência de Conhecimento pelo CONTRATANTE, a CONTRATADA terá o **prazo de 7 (sete) dias corridos** para o início dos respectivos serviços;

1.2.2.12 A CONTRATADA terá o **prazo máximo de 30 (trinta) dias corridos**, contados a partir da emissão da Ordem de Serviço específica para a Transferência de Conhecimento, para concluir ou, minimamente, disponibilizar todo o material referente à capacitação;

1.2.2.13 Para fins de ateste do serviço de suporte técnico mensal serão observados os seguintes prazos:

1.2.2.13.1 A CONTRADA deverá emitir, ao final de cada período mensal, relatório detalhado constando a relação consolidada de chamados técnicos e encaminhá-lo ao CONTRATATE **em até 5 (cinco) dias úteis** contados do fechamento do período mensal;

1.2.2.13.2 A Equipe de Fiscalização Técnica ou o Gestor do Contrato farão, mensalmente, a emissão do Termo de Recebimento Provisório, mediante a entrega do relatório detalhado de chamados técnicos, o qual deverá ser elaborado e encaminhado pela CONTRATADA ao CONTRATANTE, **em até 3 (três) dias úteis** contados do seu recebimento;

1.2.2.13.3 O Gestor do Contrato fará a emissão do Termo de Recebimento Definitivo, mediante elaboração de Termo Circunstanciado, referente ao período mensal de prestação do serviço de suporte técnico, **em até 7 (sete) dias úteis** após a emissão do Termo de Recebimento Provisório;

1.2.2.14 A CONTRATADA deverá apresentar garantia de execução contratual em uma das modalidades previstas no art. 96 da Lei nº 14.133/2021 **em até 20 (vinte) dias úteis** contados da assinatura do contrato;

1.2.2.15 O CONTRATANTE realizará a abertura de chamados de suporte técnico junto a CONTRATADA em formato 24x7, isto é, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana);

1.2.2.16 Quando peças ou componentes dos *appliances* físicos apresentarem defeito, a CONTRATADA deverá substituí-los dentro dos prazos estipulados de acordo com a categorização do nível de criticidade do componente, conforme Tabela - item 1.7.4.14.1.

1.2.2.17 Nos casos em que não seja possível o reparo dentro do prazo estipulado no item anterior, substituir **no prazo máximo de 72 (setenta e duas) horas**, em caráter temporário ou definitivo, o equipamento defeituoso por outro de mesma marca e modelo, ou superior, e com as mesmas características técnicas, novo e de primeiro uso.

1.2.2.18 Para os prazos de atendimento dos chamados técnicos em geral, deverá ser observada a definição dos Níveis Mínimos de Serviço apresentados na Tabela - item 1.7.4.14.1.

1.2.3 Requisitos técnicos

1.2.3.1 O detalhamento dos requisitos técnicos para a presente contratação está disposto no ANEXO I – Detalhamento dos requisitos técnicos do objeto para o Grupo 1, referente à solução composta por *appliances* físicos, bem como no ANEXO II – Detalhamento dos requisitos técnicos do objeto para o Grupo 2, referente à solução composta por *appliances* virtuais.

1.2.4 Requisitos de suporte

1.2.4.1 Todos os requisitos de suporte serão aplicados para ambos os tipos de solução, seja ela composta por *appliances* físicos ou virtuais, salvo quando houver diferenciação expressamente escrita;

1.2.4.2 Os serviços de suporte deverão ser capazes de atender às demandas de compatibilidade da solução ADC com a infraestrutura computacional existente no CONTRATANTE;

1.2.4.3 O serviço de suporte técnico para todos os componentes da solução deverá ser executado pela CONTRATADA, durante toda a vigência contratual, contados a partir da data de emissão do Termo de Recebimento Definitivo (TRD), referente à entrega, instalação e configuração completa da solução;

1.2.4.4 O serviço de suporte técnico da solução consistirá em:

1.2.4.4.1 Atuar, de maneira presencial, no caso da solução composta por *appliances* físicos, ou de maneira remota, no caso da solução composta por *appliances* virtuais, de forma a atender às requisições e incidentes que vierem a ocorrer na solução adquirida pelo CONTRATANTE;

1.2.4.4.2 Atuar, mediante abertura de chamado técnico pelo CONTRATANTE, na solução ADC adquirida, visando a resolução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução, permitindo o retorno à condição normal de operação;

1.2.4.4.3 Atuar, mediante abertura de chamado técnico pelo CONTRATANTE, por meio de contato telefônico ou outro recurso de comunicação, visando o esclarecimento de dúvidas em relação a qualquer elemento da solução;

1.2.4.4.4 Realizar visitas técnicas preventivas no local de instalação da solução composta por *appliances* físicos, com frequência mensal, e **com pelo menos 1 (uma) hora de duração** por visita, visando a inspeção e a garantia do correto funcionamento e o melhor desempenho da solução;

1.2.4.4.5 De maneira análoga, realizar inspeções técnicas de maneira remota no caso da solução composta por *appliances* virtuais, com frequência mensal, e **com pelo menos 1 (uma) hora de duração** por visita, visando a inspeção e a garantia do correto funcionamento e o melhor desempenho da solução;

1.2.4.4.6 Substituir peças e componentes, cujos problemas sejam decorrentes do desgaste pelo uso normal dos equipamentos, por outras de configuração idêntica ou superior, originais e novas, conforme previsto na garantia da solução e requisitos temporais correspondentes;

1.2.4.4.7 Atualizar a solução, sempre que solicitado pela CONTRATANTE, quando do lançamento de novas versões ou

de *firmwares* que corrijam vulnerabilidades conhecidas ou defeitos do software ou hardware.

1.2.4.5 O CONTRATANTE poderá realizar a abertura de chamados de suporte técnico por ligação telefônica, por *e-mail* ou via Portal da Internet (página web), em período integral, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana. Todas as três alternativas citadas deverão ser disponibilizadas e sustentadas pela CONTRATADA durante toda a vigência contratual;

1.2.4.5.1 A CONTRATADA deverá informar no documento do Plano de Implantação os procedimentos e os canais disponíveis para abertura de chamados de suporte técnico;

1.2.4.5.2 Se a Central de Suporte Técnico da CONTRATADA estiver localizada fora de Brasília-DF, deverá ser informado o DDG (discagem direta gratuita 0800);

1.2.4.5.3 O acesso à área restrita de suporte técnico em Portal da Internet da CONTRATADA deverá estar disponível, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana;

1.2.4.6 A CONTRATADA deverá enviar mensalmente, conforme estabelecido no item 1.7.2.13.1, ou disponibilizar acesso por meio do Portal da Internet, a relação consolidada dos chamados abertos no período mensal, mencionando minimamente o seguinte: número do chamado técnico, data e hora de abertura do chamado, responsável pela abertura do chamado, problemas relatados, problemas verificados pelo técnico da Contratada durante a resolução do chamado, medidas adotadas para a resolução dos problemas, eventuais pendências a serem solucionadas pelo CJF e nome do técnico responsável pelo atendimento;

1.2.4.7 A CONTRATADA deverá disponibilizar acesso a base de conhecimento do fabricante relativa aos componentes que constituem a solução adquirida, contemplando toda a documentação técnica (guias de instalação e configuração atualizados, FAQ, com pesquisa efetuada através de ferramentas de busca) e atualizações. Esta ação deverá ser realizada quando da fase de instalação e configuração da solução e será um item a ser observado quando da emissão do TRD;

1.2.4.8 A CONTRATADA deverá realizar, a cada ocorrência, como escopo das atividades de visitas técnicas preventivas, as tarefas de coleta e análise de logs dos produtos, realizar o levantamento de configurações aplicadas nos equipamentos e software embarcados na solução, buscando compará-las às melhores práticas e recomendações do fabricante, avaliar aspectos de segurança e desempenho da solução, finalizando com a elaboração de relatório técnico com as informações coletadas e as recomendações a serem aplicadas para a melhoria de desempenho, funcionalidade e segurança da solução;

1.2.4.9 Para o disposto no item anterior, o técnico da CONTRATADA deverá levar em consideração a realidade do ambiente de servidores e aplicações do CJF (*as-is*), visando otimizar o funcionamento da solução por meio de ações que atendam às necessidades e aos objetivos do CONTRATANTE (*to-be*);

1.2.4.10 As visitas técnicas/inspeções preventivas deverão ser realizadas por técnico(s) plenamente qualificado(s), com certificação emitida pelos fabricantes dos equipamentos da solução ofertada, e deverão ser realizadas sempre com acompanhamento da equipe técnica do CONTRATANTE;

1.2.4.11 A contagem de prazo para a realização das visitas /inspeções técnicas preventivas será iniciada após emissão do Termo de Recebimento Definitivo, devendo ocorrer automaticamente em dia e hora previamente agendada com o CONTRATANTE e serão consideradas concluídas após o entrega do relatório técnico de atendimento e aceite pelo CONTRATANTE. A cada visita/inspeção deverá ser gerado relatório técnico com sugestões e ajustes para a melhoria de desempenho, funcionalidade e segurança;

1.2.4.12 A CONTRATADA deverá prestar as informações e os esclarecimentos que venham a ser solicitados pela equipe técnica do CONTRATANTE, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações.

1.2.4.13 O serviço de suporte técnico especializado deverá ser prestado por localidade, de acordo com o CONTRATANTE, independente do quantitativo de equipamentos a serem fornecidos/implantados no site. Dessa forma, tal serviço não deverá ser majorado ou ajustado em casos de aquisições “tardias ou pontuais”.

1.2.4.14 Os chamados de suporte técnico abertos pelo CONTRATANTE deverão ser categorizados em 3 (três) níveis, da seguinte forma:

1.2.4.14.1 – Descrição dos Níveis Mínimos de Serviço aplicados ao serviço de suporte técnico

Criticidade	Descrição	Prazo máximo para início de atendimento (contados a partir da abertura do chamado)	Prazo máximo para restauração do serviço (contados a partir da abertura do chamado)

Severidade 1 (Alta)	Atuação ON-SITE em ocorrências que causem indisponibilidade ou restrição de funcionalidade da solução prejudicando a operação normal e que gerem impacto ao negócio.	Em até 2 (duas) horas deve ter um técnico da CONTRATADA ON-SITE.	Em até 4 (quatro) horas
Severidade 2 (Média)	Atuação REMOTA visando sanar problemas que criem restrições a operação normal da solução não gerando impacto ao negócio.	Em até 6 (seis) horas um técnico da CONTRATADA entra em contato.	Em até 12 (doze) horas
Severidade 3 (Baixa)	Atuação REMOTA visando sanar problemas que não afetem a operação normal da solução ou dúvidas de operação e configuração.	Em até 12 (doze) horas um técnico da CONTRATADA entra em contato.	Em até 36 (trinta e seis) horas

1.2.4.14 O não atendimento aos Níveis Mínimos de Serviço estabelecidos anteriormente acarretará aplicação de glosa sobre o custo mensal do serviço de suporte técnico, o qual será mais bem detalhado no item 4.10 deste Termo de Referência.

1.2.5 Requisitos de capacitação

1.2.5.1 A CONTRATADA deverá realizar a ação de Transferência de Conhecimento, preferencialmente de maneira remota, para o quantitativo de pessoas estabelecido por cada órgão partícipe do presente Sistema de Registro de Preços - SRP;

1.2.5.2 O serviço de transferência de conhecimento será solicitado sob demanda, a partir da data inicial de vigência da contratação, será solicitado sob demanda. Cada órgão partícipe do presente SRP emitirá a sua Ordem de Serviço, de maneira individualizada, para dar início à ação de Transferência de Conhecimento;

1.2.5.3 Havendo o interesse, um ou mais órgãos partícipes poderão combinar de realizar a ação de Transferência de Conhecimento de forma conjunta e integrada, desde que respeitados os prazos estabelecidos no Termo de Referência, cabendo à CONTRATADA a organização das turmas;

1.2.5.4 O treinamento deverá ter **carga horária mínima de 40 (quarenta) horas**;

1.2.5.5 O treinamento deverá ser realizado no formato *online*, em plataforma a ser definida e disponibilizada pela CONTRATADA;

1.2.5.6 O treinamento deverá ser realizado sempre em um único turno, preferencialmente o vespertino, de cada dia agendado;

1.2.5.7 A CONTRATADA deverá fornecer o conteúdo didático utilizado no treinamento para todos os participantes;

1.2.5.7.1 O material didático da transferência de conhecimento deverá ser disponibilizado em formato eletrônico, sem custo adicional para o CONTRATANTE, devendo ainda estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), tendo em vista que é comum soluções de Tecnologia da Informação serem desenvolvidas por empresas estrangeiras e material bilíngue;

1.2.5.8 Caberá à CONTRATADA o controle de participação no treinamento pelos servidores indicados pelo CONTRATANTE e, ao final, deverá entregar ao gestor do contrato a lista de presença dos participantes indicados;

1.2.5.9 Ao final da ação de Transferência de Conhecimento, a CONTRATADA deverá emitir certificado de participação para cada um dos participantes capacitados, detalhando o seguinte:

1.2.5.9.1 Nome da instituição de ensino (caso aplique-se);

1.2.5.9.2 Nome do curso/capacitação (caso aplique-se);

1.2.5.9.3 Nome completo do aluno capacitado;

1.2.5.9.4 Data de início e término da capacitação;

1.2.5.9.5 Carga horária;

1.2.5.9.6 Conteúdo programático (Ementa).

1.2.5.10 O instrutor designado para a ação de treinamento deverá possuir certificação emitida pelo fabricante dos *appliances* ADC, ou, alternativamente, poderá ser um profissional que atuou na etapa de instalação e configuração da solução no CONTRATANTE;

1.2.5.10.1 No caso de o instrutor não ter participado da etapa de instalação e configuração da solução no CONTRATANTE, a comprovação da certificação deverá ser apresentada até 1 (um) dia antes do início da ação de treinamento;

1.2.5.11 O programa para a transferência de conhecimento deverá abordar as principais funcionalidades de administração e operação da solução e ser previamente aprovado pelo CONTRATANTE, e eventuais mudanças de conteúdo solicitadas deverão constar no material didático;

1.2.5.12 O programa deverá abordar funcionalidades da solução na versão fornecida, em especial:

1.2.5.12.1 Apresentação da arquitetura da solução e dos conceitos fundamentais;

1.2.5.12.2 Aspectos sobre instalação da solução;

1.2.5.12.3 Configuração e gerenciamento da solução;

1.2.5.12.4 Operação completa da solução;

1.2.5.12.5 Análise de logs e problemas;

1.2.5.12.6 Geração e customização de relatórios, caso aplicável;

1.2.5.12.7 Verificação de alertas e tomada de ações;

1.2.5.12.8 Deduplicação de dados;

1.2.5.12.9 Segurança da Informação e da solução;

1.2.5.12.10 Otimizações ou desempenho (performance);

1.2.5.12.11 Troubleshooting.

1.2.5.13 A CONTRATADA deverá realizar laboratórios práticos que permitam exercitar os conteúdos acima.

1.2.5.14 O cronograma efetivo da ação de Transferência de Conhecimento será definido em conjunto com o CONTRATANTE quando da realização da Reunião Inicial de Planejamento;

1.2.5.15 Caso a Transferência de Conhecimento não seja satisfatória com relação à profundidade do conteúdo apresentado ou domínio dos temas por parte do instrutor, a CONTRATADA deverá complementar, sem ônus adicional, o repasse dos pontos considerados pelo CONTRATANTE como insatisfatórios.

1.2.5.16 A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes dos softwares e equipamentos da solução ofertada.

1.2.6 Requisitos de sustentabilidade ambiental (Art. 18, § 1º, XII, da Lei n. 14.133/2021)

1.2.6.1 A CONTRATADA será responsabilizada por qualquer prejuízo que venha causar ao CJF em virtude de ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ligadas aos produtos e serviços objeto do presente Termo de Referência.

1.2.6.2 A CONTRATADA deverá, para a execução dos serviços, fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços, conforme disposto no art. 6º, inciso IV, da Instrução Normativa SLTI/MPOG n. 01, de 19 de janeiro de 2010;

1.2.6.3 A CONTRATADA deverá comprovar que bens ofertados atendem aos critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos no art. 3º, II, do Decreto n. 7.174, de 12 de maio de 2010 e pela Portaria INMETRO n. 170, de 10 de abril de 2012.

1.2.6.4 A comprovação do item anterior, quando solicitada pela Administração, poderá ser feita mediante apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, ou ainda por qualquer outro meio de prova, inclusive declaração voluntária, que ateste que os bens fornecidos cumprem com as exigências, conforme o art. 42, I e III, da Lei n. 14.133, de 1º de abril de 2021.

1.2.6.5 A CONTRATADA deverá observar, sempre que possível, para a entrega dos produtos adquiridos, as normas em vigor atinentes à sustentabilidade e ao Manual de Sustentabilidade nas compras e contratações do Conselho da Justiça Federal, instituído pela Portaria CJF n. 96, de 10 de fevereiro de 2023.

1.2.6.6 A CONTRATADA deverá respeitar a legislação vigente e as normas técnicas elaboradas pela ABNT e pelo INMETRO para aferição e garantia de aplicação dos requisitos mínimos de qualidade e segurança dos produtos adquiridos neste Termo de Referência.

1.2.7 Requisitos legais e normativos aplicáveis ao objeto da contratação

1.2.7.1 Resolução CNJ n. 396/2021: Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

1.2.7.2 Resolução CNJ n. 468/2022: Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça.

1.2.7.3 Resolução CJF n. 06/2008: Alterada pela Resolução CJF n. 687, de 15 de dezembro de 2020, que dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2º graus;

1.2.7.4 Portaria CJF n. 232/2023: Dispõe sobre as etapas do planejamento da contratação, para aquisição de bens e contratações de serviços sob o regime de execução indireta, no âmbito do Conselho da Justiça Federal.

1.3. Descrever solução de TIC de forma detalhada, motivada e justificada (considerado todo o ciclo de vida do objeto)

1.3.1 Descrição dos itens que compõem o GRUPO 1 do objeto

1.3.1.1 O GRUPO 1 do objeto desta contratação é referente à solução de *Application Delivery Controller* – ADC constituída por *appliances* físicos (equipamentos) com *hardware* específico para desempenhar as funções desejadas, conforme requisitos de negócio e requisitos técnicos especificados no Estudo Técnico Preliminar, inclusive quanto a necessidade de aquisição de marca e modelo compatíveis com os em uso no STJ (fabricante F5, modelo BIG-IP R4800).

1.3.1.2 Além disso, integram o GRUPO 1 toda a cadeia de serviços decorrentes da solução adquirida, necessários à sustentação e continuidade dos serviços durante a vigência contratual. Este grupo constitui a solução escolhida pelo CJF e pelos TRFs da 3ª e 6ª Região.

a) Item 1.1 – *Appliance* físico para solução ADC: Consiste em 1 (um) *appliance* físico do fabricante F5, Modelo BIG-IP R4800, incluindo *softwares* embarcados e todos os acessórios necessários à instalação do equipamento, conforme especificações técnicas presentes no ANEXO I deste documento. Deve-se considerar ainda que a marca e o modelo são os adotados pelo STJ, sendo, portanto, necessária a aquisição pelo CJF da mesma marca e modelo ou de similares compatíveis e de qualidade superior

b) Item 1.2 – Serviço de instalação e configuração da solução ADC: Consiste no serviço de instalação e configuração da solução adquirida no ambiente do CONTRATANTE, conforme suas necessidades e observando-se o cronograma constante do ANEXO IV. Cada unidade deste serviço é referente a 1 (uma) unidade adquirida do *appliance* físico constante do item 1.1 do objeto;

c) Item 1.3 – Serviço de garantia e suporte técnico presencial para a solução ADC: Serviço de garantia dos equipamentos que compõem a solução e suporte técnico prestado de maneira presencial durante os 60 (sessenta) meses de vigência contratual e durante eventual prorrogação do contrato. Também inclui visita técnica obrigatória a cada período mensal para análise, geração de relatórios de desempenho e sugestão de melhorias da solução. Este serviço será iniciado imediatamente após a emissão do Termo de Recebimento Definitivo do Serviço de instalação e configuração da solução e se encerrará juntamente com o término da vigência contratual. Ele engloba toda a solução adquirida e será pago mensalmente, estando sujeito à avaliação de Níveis Mínimos de Serviço para aferição do desempenho da CONTRATADA;

d) Item 1.4 – Transferência de conhecimento: Serviço referente à ação de Transferência de Conhecimento, a ser realizada durante a vigência contratual, a partir da data inicial de vigência da contratação, mediante emissão de Ordem de Serviço específica expedida pelo CONTRATANTE. Será realizada *online*, com material didático no formato eletrônico, carga horária mínima de 40 (quarenta) horas, com entrega de certificado aos participantes e destinada a capacitar a equipe técnica do CONTRATANTE para compreender, operar e gerenciar a solução adquirida;

e) Item 1.5 – Serviços técnicos especializados para implementação e customização da solução ADC: Serviço técnico especializado de implementação e customização da solução ADC, a ser utilizado sob demanda, mediante Ordem de Serviço expedida pelo CONTRATANTE e sem garantia mínima de utilização durante a vigência contratual. Esse serviço será destinado a realizar implementações e customizações na solução ADC de acordo com as necessidades e requisitos do CONTRATANTE. Assim, o serviço será utilizado para evoluir e aprimorar a solução, conforme melhor entendimento do corpo técnico do CONTRATANTE.

1.3.2 Descrição dos itens que compõem o GRUPO 2 do objeto

1.3.2.1 O GRUPO 2 do objeto desta contratação é referente à solução de *Application Delivery Controller* – ADC constituída por *appliances* virtuais: *softwares* instalados em servidores de rede para desempenhar as funções desejadas, conforme requisitos de negócio e requisitos técnicos especificados no Estudo Técnico Preliminar.

1.3.2.2 Além disso, integram o GRUPO 2 toda a cadeia de serviços decorrentes da solução adquirida, necessários à sustentação e continuidade dos serviços durante a vigência contratual. Este grupo constitui a solução escolhida exclusivamente pelo TRF da 5ª Região.

a) Item 2.1 – *Appliance* virtual para solução ADC – Tipo 1: Consiste em 2 (duas) unidades virtuais de *appliance* ADC – *Application Delivery Controller*, do Tipo 1, conforme especificações técnicas presentes no ANEXO II. Este item inclui todos os licenciamentos/subscrições dos *softwares* que compõem a solução virtual pelo prazo de 60 (sessenta) meses;

- b) Item 2.2 – *Appliance* virtual para solução ADC – Tipo 2: Consiste em 2 (duas) unidades virtuais de *appliance* ADC – *Application Delivery Controller*, do Tipo 2, conforme especificações técnicas presentes no ANEXO II. Este item inclui todos os licenciamentos/subscrições dos *softwares* que compõem a solução virtual pelo prazo de 60 (sessenta) meses;
- c) Item 2.3 – Serviço de instalação e configuração da solução ADC: Consiste no serviço de instalação e configuração da solução adquirida no ambiente do CONTRATANTE, conforme suas necessidades e observando-se o cronograma constante do ANEXO IV. Cada unidade deste serviço é referente a 1 (uma) unidade adquirida dos *appliances* virtuais constantes dos itens item 2.1 e item 2.2 do objeto;
- d) Item 2.4 – Serviço de suporte técnico remoto para a solução ADC: Serviço de suporte técnico prestado de maneira remota durante os 60 (sessenta) meses de vigência contratual. Também inclui inspeção técnica obrigatória a cada período mensal para análise, geração de relatórios de desempenho e sugestão de melhorias da solução. Este serviço será iniciado imediatamente após a emissão do Termo de Recebimento Definitivo do Serviço de instalação e configuração da solução e se encerrará juntamente com o término da vigência contratual. Ele engloba toda a solução adquirida e será pago mensalmente, estando sujeito à avaliação de Níveis Mínimos de Serviço para aferição do desempenho da CONTRATADA;
- e) Item 2.5 – Transferência de conhecimento: Serviço referente a ação de Transferência de Conhecimento, a ser realizada durante a vigência contratual, mediante emissão de Ordem de Serviço específica espedida pelo CONTRATANTE. Será realizada *online*, com material didático no formato eletrônico, carga horária mínima de 40 (quarenta) horas, com entrega de certificado aos participantes e destinada a capacitar a equipe técnica do CONTRATANTE para compreender, operar e gerenciar a solução adquirida;
- f) Item 2.6 – Serviços técnicos especializados para implementação e customização da solução de ADC: Serviço técnico especializado de implementação e customização da solução ADC, a ser utilizado sob demanda, mediante Ordem de Serviço espedida pelo CONTRATANTE e sem garantia mínima de utilização durante a vigência contratual. Esse serviço será destinado a realizar implementações e customizações na solução ADC de acordo com as necessidades e requisitos do CONTRATANTE. Assim, o serviço será utilizado para evoluir e aprimorar a solução, conforme melhor entendimento do corpo técnico do CONTRATANTE.

1.4. Ciclo de vida do objeto

1.4.1. Item 1 - Bens: Solução ADC – Fabricante F5, Modelo BIG-IP R4800

a) No processo de aquisição conjunta dos dois ADCs é fundamental considerar o ciclo de vida de bens e produtos. Este ciclo engloba as etapas de produção, distribuição, armazenamento, utilização e descarte. Cada uma dessas fases requer a definição de indicadores que permitam monitorar a eficácia do processo de compra e a sustentabilidade de cada etapa.

1.4.1.1. Produção:

1.4.1.1.1 Considera-se, nesta fase, o compromisso do fabricante com práticas sustentáveis e a conformidade com as normas ROHS (*Restriction of Certain Hazardous Substances*). Além disso, é imprescindível que os equipamentos apresentem um consumo de energia reduzido, respeitando padrões internacionais de sustentabilidade para produtos de informática. Por fim, é preciso que os equipamentos sejam projetados para serem facilmente reparáveis e atualizados.

1.4.1.1.2 Alguns indicadores usados para esta fase podem ser:

- a) Índice de eficiência energética: medida do consumo de energia do produto em relação ao padrão da indústria.
- b) Conformidade com normas ambientais: percentual de conformidade com normas internacionais de sustentabilidade.

1.4.1.2. Distribuição:

1.4.1.2.1 A fase de distribuição desempenha um papel crucial na cadeia de suprimentos de qualquer produto, particularmente no que se refere ao impacto ambiental e à eficiência da entrega.

1.4.1.2.2 Um indicador usado para esta fase pode ser:

- a) Tempo médio de entrega: tempo que leva para cada equipamento ADC ser entregue.

1.4.1.3. Armazenamento:

1.4.1.3.1 Esta fase trata do armazenamento dos ADCs até que sejam instalados e configurados. As condições de armazenamento devem ser adequadas para preservar a integridade dos equipamentos.

1.4.1.3.2 Alguns indicadores usados para esta fase podem ser:

- a) Índice de condições de armazenamento: avaliação das condições de armazenamento em termos de temperatura, umidade e segurança.

- b) Capacidade de armazenamento: volume e localização disponíveis para o armazenamento dos ADCs.
- c) Índice de segurança do armazenamento: grau de segurança do local de armazenamento, considerando fatores como sistemas de segurança física, sistemas de monitoramento e proteção contra incêndio e inundações.

1.4.1.4. Utilização:

1.4.1.4.1 Durante a fase de utilização, é fundamental assegurar que os ADCs funcionem eficientemente, com manutenção regular para prolongar sua vida útil e evitar falhas. Cabe dizer que, a vida útil média de equipamentos de rede de alta performance como o F5 BIG-IP R4800 é de 5 a 7 anos. Essa estimativa é baseada na experiência com equipamentos de rede de classe empresarial, onde a longevidade é determinada pela durabilidade dos componentes e pelo suporte contínuo do fabricante.

1.4.1.4.2 Alguns indicadores usados para esta fase podem ser:

- a) Tempo médio entre falhas: tempo médio entre as falhas de hardware. Quanto maior este tempo, mais confiável é o sistema.
- b) Tempo médio para reparos: tempo médio necessário para reparar os equipamentos após uma falha.

1.4.1.5. Descarte:

1.4.1.5.1 A fase de descarte é a última fase do ciclo de vida dos equipamentos. Dada a complexidade e o ritmo acelerado da tecnologia, é essencial planejar o fim do ciclo de vida dos equipamentos, de modo a minimizar o impacto ambiental, assegurar a conformidade com as normas de resíduos eletrônicos e maximizar o valor residual dos equipamentos.

1.4.1.5.2 Nesta fase de descarte, é necessário cumprir as normativas estabelecidas na Resolução CJF 462, de novembro de 2017, que dispõe sobre a administração de bens móveis no âmbito do CJF e da Justiça Federal de 1º e 2º graus. Nessa esteira, a sugestão é pelos seguintes indicadores:

- a) Valor residual dos ADCs: valor residual dos equipamentos no momento do descarte. Embora esse não seja um parâmetro utilizado na Resolução CJF 462/2017, isso seria um parâmetro de comparação com outros modelos usualmente adquiridos pelas unidades.
- b) Taxa de reutilização: porcentagem de equipamentos realocados e reutilizados internamente após atingirem o fim do seu ciclo de vida inicial. Uma taxa de reutilização mais alta sugere que os equipamentos continuam funcionando de maneira eficaz e que os recursos da organização estão sendo otimizados.

1.4.2. Itens 2 e 3 – Serviços: Instalação e configuração, garantia e suporte da solução ADC

1.4.2.1. Planejamento:

1.4.2.1.1 As especificações do suporte técnico necessário devem ser claramente definidas e os requisitos técnicos para a instalação e configuração do ADC devem ser cuidadosamente articulados para garantir que os possíveis licitantes tenham uma compreensão clara do escopo do contrato.

1.4.2.1.2 Alguns indicadores usados para esta fase podem ser:

- a) Dimensionamento de necessidades: precisão com que a unidade demandante avalia as necessidades de suporte considerando tanto o presente quanto o futuro.
- b) Equipamentos de segurança: como a empresa contratada será responsável por fornecer os equipamentos de segurança necessários para a execução dos serviços, é importante incluir no edital de licitação detalhes claros sobre as expectativas em relação a esses equipamentos. O indicador poderia ser a adequação e a conformidade desses equipamentos com as normas de segurança vigentes.
- c) Preparação para possíveis riscos e contingências: avaliar a preparação do plano de licitação para possíveis riscos e contingências. Isso poderia ser medido considerando a inclusão de cláusulas de gestão de riscos e contingências no edital.

1.4.2.2. Contratação:

1.4.2.2.1 A licitação é publicada e os licitantes potenciais são convidados a apresentar suas propostas. As propostas são então avaliadas com base nos critérios estabelecidos no plano de licitação, tais como a experiência do licitante no fornecimento de suporte técnico para o software em questão, a qualidade do serviço proposto e o preço.

1.4.2.2.2 Um indicador usado para esta fase pode ser:

- a) Qualidade das propostas recebidas: número de propostas que atendem aos critérios estabelecidos.

1.4.2.3. Prestação do serviço:

1.4.2.3.1 Uma vez que a licitação é concedida a um fornecedor, o contrato entra em sua fase de execução. Após a adjudicação do contrato, o fornecedor começa a execução dos serviços de instalação e configuração do ADC, além de fornecer suporte técnico conforme especificado no contrato.

1.4.2.3.2 Alguns indicadores usados para esta fase podem ser:

- a) Tempo de resposta: tempo necessário para que a equipe de suporte técnico responda a uma solicitação de serviço. Este é um aspecto crítico da execução do serviço de suporte técnico.
- b) Taxa de resolução na primeira chamada: percentual de chamadas de suporte ou tickets resolvidos na primeira interação com a equipe de suporte técnico.
- c) Satisfação do usuário: satisfação dos usuários finais com o serviço de suporte técnico.
- d) Tempo de resolução: tempo médio que a equipe de suporte leva para resolver um problema depois que ele foi relatado.
- e) Escalabilidade do suporte: capacidade do serviço de suporte de lidar com um aumento no volume de solicitações ou complexidade dos problemas sem comprometer a qualidade do serviço.
- f) Manutenção preventiva: quantidade e efetividade das ações de manutenção preventiva realizadas para evitar problemas futuros.

1.4.2.4. Avaliação e encerramento:

1.4.2.4.1 No final do contrato, é necessário realizar uma revisão para avaliar a eficácia do suporte técnico fornecido e determinar se os objetivos do contrato foram alcançados. Se o serviço foi satisfatório e ainda há necessidade de suporte técnico, o contrato pode ser renovado. Caso contrário, o contrato é encerrado e um novo ciclo de licitação pode ser iniciado.

1.4.2.4.2 Alguns indicadores usados para esta fase podem ser:

- a) Taxa de recorrência de problemas: quantos problemas resolvidos reaparecem. Uma alta taxa de recorrência pode indicar uma abordagem de "correção de sintomas" ao invés de "correção de causas raiz", o que é insustentável a longo prazo.
- b) Melhorias contínuas: quantidade e a efetividade das melhorias propostas e implementadas durante o período do contrato.
- c) Transferência de conhecimento: ao final do contrato, o fornecedor deve ter transferido conhecimento suficiente para a equipe de TI sem a necessidade de suporte externo constante. Este indicador pode ser medido pela competência da equipe interna no final do contrato.

1.4.3. Item 4 – Serviço: Transferência de conhecimento

a) Considerando a singularidade e a complexidade da oferta do serviço alvitrada, torna-se crucial para o Conselho da Justiça Federal a realização de uma avaliação da qualidade do curso ofertado. Essa análise cumpre com os mandatos legais previstos no artigo 18, inciso VIII, da Lei 14.133/2021, sublinhando a importância de uma gestão efetiva e criteriosa de contratação.

1.4.3.1. Planejamento:

1.4.3.1.1 Nesta fase, ocorre o reconhecimento de uma exigência específica por parte da unidade demandante, seguido pelo desenvolvimento criterioso da prestação de um serviço destinado a atender às necessidades de cada um dos servidores da TI. Deste modo, é preciso destacar a elaboração de estratégias e métodos para garantir a prestação eficiente dos serviços contratados, além da alocação dos recursos necessários para sua execução, infraestrutura adequada e tecnologia necessária.

1.4.3.1.2 Alguns indicadores usados para esta fase podem ser:

- a) Experiência profissional precedente dos servidores da TI: experiência profissional dos beneficiários da instrução correlacionada à pertinência e aplicabilidade do conteúdo dos cursos ofertados.
- b) Competências específicas a serem desenvolvidas: competências a serem desenvolvidas alinhadas às necessidades imediatas do trabalho e aos objetivos estratégicos deste Conselho da Justiça Federal.

1.4.3.2. Contratação:

1.4.3.2.1 A fase de contratação é crítica, pois estabelece as bases legais e operacionais para a prestação de um serviço

essencial. No contexto da contratação por inexigibilidade para fornecer treinamento na modalidade de Educação a Distância, a relevância dessa fase é ainda maior, considerando a necessidade de capacitação contínua e de qualidade dos servidores da TI peritos.

1.4.3.2.2 Alguns indicadores usados para esta fase podem ser:

- a) Adesão ao cronograma: mede a eficiência do processo de contratação ao seguir o cronograma de entrega de documentação, entre outros aspectos necessários, indicando se a contratação foi realizada dentro do prazo planejado.
- b) Custo-benefício: analisa se a contratação está alinhada com os benefícios previstos, incluindo a qualidade e a diversidade das instruções previstas.

1.4.3.3. Prestação de serviço:

1.4.3.3.1 A fase de prestação do treinamento vai além da simples realização de atividades, emergindo como um ponto crítico onde os benefícios concretos são gerados e mensurados. No caso específico de um curso online, a execução do serviço abarca diversas facetas: desde a seleção cuidadosa e apresentação do material didático até o acompanhamento e desenvolvimento dos participantes.

1.4.3.3.2 Alguns indicadores usados para esta fase podem ser:

- a) Qualidade do material didático fornecido: este indicador pode ser avaliado por meio da revisão por pares especializados e ainda por meio de feedback direto dos servidores da TI beneficiários da instrução.
- b) Feedback dos servidores da TI beneficiários da instrução sobre a plataforma de ensino: eficácia dos sistemas fornecidos pela empresa contratada como ferramentas educativas.
- c) Uso de recursos de aprendizagem adicionais: engajamento dos servidores da TI beneficiários da instrução com materiais suplementares como leituras complementares, vídeos adicionais, e fóruns de discussão especializados.
- d) Desenvolvimento de competências alvo: grau em que as competências específicas foram desenvolvidas entre os servidores da TI ao término do curso.

1.4.3.4. Avaliação e Encerramento:

1.4.3.4.1 Ao concluir a contratação, iniciam-se as fases de avaliação e encerramento, onde se verifica se o treinamento atendeu aos critérios estabelecidos e se todos os serviços foram prestados conforme o contrato. Essa etapa é crucial, pois além de garantir que os objetivos foram alcançados, envolve também a coleta e avaliação dos feedbacks dos servidores da TI participantes. Este retorno é essencial, pois reflete a eficácia da instrução e fornece insights fundamentais para a melhoria de contratações futuras e a análise da viabilidade de parcerias educacionais continuadas no Conselho. Com isso, a equipe de gestão do programa tem a responsabilidade de compilar estas avaliações, integrar os comentários recebidos e aplicar as devidas medidas para aperfeiçoar os futuros ciclos de treinamento.

1.4.3.4.2 Alguns indicadores usados para esta fase podem ser:

- a) Índice de satisfação dos servidores da TI beneficiários da instrução: este indicador qualitativo pode ser desmembrado em várias subcategorias, como "Clareza do conteúdo", "Usabilidade da plataforma" e "Valor geral percebido". Cada subcategoria pode ser avaliada utilizando uma escala Likert, por exemplo.
- b) Avaliação do desempenho docente: aqui, a métrica deve ser mais granular, avaliando a eficiência dos instrutores contratados em diferentes aspectos como "Disponibilidade para esclarecimento de dúvidas", "Habilidade em facilitar discussões" e "Inovação pedagógica".
- c) Índice de aplicabilidade prática: grau de transferência de habilidades aplicáveis à função ou carreira dos servidores da TI beneficiários da instrução.

2. Fundamentação da contratação (Art. 6º, XXIII, "b" c/c art. 18, §1º, I e II, Lei n. 14.133/2021)

2.1. Motivação da contratação (Art. 5º, Lei n. 14.133/2021)

2.1.1 Motivação por parte do CJF

2.1.1.1 No cenário anteriormente descrito, as informações armazenadas e disponibilizadas, as quais trafegam pela Internet, tornam-se alvo de criminosos cibernéticos. Nos últimos anos, houve um crescimento exponencial de ataques cibernéticos que, com o advento das ferramentas de inteligência artificial e o poder de processamento distribuído, tendem a se tornar cada vez mais agressivos. Vários órgãos do Poder Judiciário sofreram ataques virtuais a partir de 2020 e uma dessas investidas foi a responsável pela paralisação das atividades judiciais do STJ, em novembro/2020

2.1.1.2 Nessa esteira, o Conselho Nacional de Justiça - CNJ emitiu a Resolução n. 396/2021, a qual institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), determinando que os órgãos do Judiciário aprimorem o seu nível de maturidade em segurança cibernética por meio de ações preparatórias (proativas) e de

remediação (corretivas), além do monitoramento constante aos seus ambientes computacionais. Tais medidas concentram-se no objetivo de tentar evitar ou mitigar os possíveis danos que esses ataques são capazes de produzir sobre as atividades jurisdicionais dos Tribunais brasileiros.

2.1.1.3 Assim, para permitir a criação de uma unidade de contingência de aplicações fora do espaço físico do CJF (*offsite*), neste projeto, pretende-se utilizar o *data center* localizado no STJ. Essa parceria entre órgãos já ocorre entre o Tribunal de Contas da União - TCU e o Tribunal Superior do Trabalho - TST e entre o Supremo Tribunal Federal - STF e o CNJ. Entre o STJ e o CJF há o Acordo de Cooperação Técnica STJ/CJF n. 01/2023, cujo objetivo é a conjugação de esforços para a implantação de sítio de contingência entre os órgãos partícipes, de forma a prover os serviços tecnológicos essenciais ao funcionamento desses órgãos. Contudo, atualmente, os termos desse Acordo de Cooperação Técnica somente são utilizados para réplica dos dados de *backup*. Faz-se, então, necessário abranger novas dimensões para implementar efetivamente o teor desse Acordo.

2.1.1.4 Como requisito para a criação do sítio de contingência, há a exigência para que o CJF duplique suas aplicações e serviços críticos e os armazene e disponibilize no *data center* localizado no STJ. Exemplos de serviços críticos seriam o DNS (*Domain Name System*) externo, Portal Institucional, sistemas nacionais, dentre outros. Para viabilizar a movimentação dos serviços entre o CJF e o STJ é necessário que os dois órgãos compartilhem infraestrutura e recursos computacionais, tais como rede, links de comunicação, *storages* (para armazenamento de dados) e ambiente de virtualização. Por conseguinte, no processo de análise de viabilidade da solução desejada, identificou-se que ambos os órgãos utilizam a mesma solução de virtualização de servidores (VMware), como a tecnologia de armazenamento de dados é idêntica, a qual (id. 0533280), e já existe um link de 10 Gbps interligando os dois edifícios-sede, provisionado por meio de contrato de prestação de serviço do STJ para acesso à rede metropolitana denominada Infovia Brasília, operada pela empresa pública SERPRO.

2.1.1.5 Ademais, em 2023, o STJ adquiriu solução de ADC composta por um conjunto de dois equipamentos iguais (processo SEI/STJ n. 043569/2022, Contrato STJ n. 108/2023), porém de fabricante diferente da solução WAF (*Web Application Firewall*) atualmente em uso no CJF (Contrato CJF n. 012/2021, processo SEI n. 0000843-22.2020.4.90.8000). Deste modo, faz-se necessário que o CJF adquira solução ADC do mesmo fabricante que o STJ, de forma que os equipamentos dos dois órgãos possam ser interligados, permitindo o balanceamento de serviços entre eles. A solução adquirida pelo STJ pertence ao fabricante F5, modelo BIG-IP R4800, enquanto o CJF utiliza equipamentos adquiridos por intermédio do Contrato CJF n. 047/2017, encerrado em março/2023, do fabricante Fortinet, modelo FortiWeb 2000E. Neste tocante, para viabilizar o projeto do sítio de contingência, os dois órgãos devem possuir solução ADC da mesma marca e categoria de desempenho, de forma que haja perfeita comunicação entre os equipamentos, sem que esbarrem em diferenças de implementação lógica ou de *hardware*, bem como não exista gargalos de desempenho devido a limitação entre suas taxas de transferência.

2.1.1.6 Em tratativas com o STJ, foi informado que aquele Tribunal também está em fase de planejamento para a implantação de sítio de contingência neste Conselho. Inicialmente, foi idealizada uma compra compartilhada dos equipamentos ADC entre os dois órgãos. Contudo, como o STJ tinha urgência na aquisição da sua solução, ainda no exercício de 2023, em razão do término da garantia da solução WAF que eles utilizavam, não foi possível ao CJF planejar a contratação conjuntamente.

2.1.1.7 Importante destacar que as funcionalidades da solução atualmente em uso no CJF e da solução recentemente adquirida pelo STJ não permitem a interligação dos equipamentos. Sendo, portanto, necessária a contratação de solução correspondente a do STJ, ou seja, solução pertencente ao fabricante F5, modelo BIG-IP R4800 ou de similares compatíveis e de qualidade superior.

2.1.1.8 Desta forma, a aquisição da solução de controle de entrega de aplicações - ADC (*Application Delivery Controller*) é motivada pela obtenção dos seguintes benefícios, os quais trarão melhorias significativas para o CJF e para toda a Justiça Federal:

- a) Melhoria no desempenho: O ADC possui mecanismos de compressão de dados, otimização de protocolos, *traffic shaping* e *SSL Offloading* que otimizam o tráfego de informações entre clientes e servidores, além de realizar a priorização para favorecer aplicações críticas;
- b) Alta disponibilidade: Ele proporciona redundância e mecanismo de *failover* (chaveamento automático entre servidores), garantindo que as aplicações estejam sempre disponíveis, mesmo em caso de falha de um servidor ou de um *data center* inteiro, pois o tráfego é redirecionado para a sítio de contingência separado geograficamente;
- c) Segurança aprimorada: O ADC pode oferecer recursos como *firewall* de aplicativos da web (WAF), proteção contra ataques de negação de serviço (DoS e DDoS), ajudando a proteger as aplicações contra ameaças cibernéticas.
- d) Balanceamento de carga: O ADC pode distribuir o tráfego de forma inteligente e equilibrada entre vários servidores, localizados no mesmo *data center* ou não, garantindo que nenhum servidor fique sobrecarregado e que as aplicações sejam entregues tempestivamente aos requisitantes.
- e) Possibilitar a escalabilidade dos sistemas: Por meio do balanceamento de carga, o ADC, em conjunto com as tecnologias de containerização já utilizadas por este CJF, permitirá que aplicações ou sistemas muito requisitados em horários de pico escalem automaticamente para suprir a demanda de requisições;

2.1.1.9 Em resumo, a contratação e implantação de uma solução ADC trará benefícios significativos para o ambiente de tecnologia em termos de desempenho, segurança e disponibilidade das aplicações, contribuindo para uma melhor

experiência do usuário e eficiência operacional de toda a Justiça Federal.

2.1.2 Motivação por parte do TRF3

2.1.2.1 Da Justificativa da Contratação

a) A Justiça Federal da 3ª Região (JF3R) busca aprimorar sua infraestrutura de tecnologia da informação, especialmente no que se refere à segurança, disponibilidade e desempenho das aplicações críticas. Atualmente este Tribunal conta com serviço de WAF em nuvem, que é capaz de mitigar ataques cibernéticos, atenuar a incidência de bots indesejados e proteger contra negação de serviço antes de a requisição maliciosa chegar no datacenter da JF3R, através de filtragem, monitoramento e bloqueio do tráfego mal-intencionado. Além disso, esta corte conta com serviços de balanceamento de carga local em software para as aplicações, tecnologia que realiza distribuição do tráfego de rede entre diversos servidores que provem determinada aplicação, otimizando a entrega da resposta, o que aumenta o desempenho da aplicação e consequentemente a satisfação dos usuários.

b) Com relação ao balanceador de carga utilizado atualmente pelo sistema chave da JF3R, o PJe, é um software open-source que realiza bem as funções que se propõe, porém com algoritmos de balanceamento simples, sem contar com uma visão holística dos nós da aplicação, que seria ideal para uma distribuição inteligente da carga de trabalho, além de não possuir um suporte técnico profissional para casos de falha.

c) Desta forma, faz-se necessário a contratação do Controlador de Entrega de Aplicações, por se tratar de uma solução completa nos quesitos segurança, escalabilidade do ambiente e melhoria no desempenho das aplicações providas pela Justiça Federal da 3ª Região. O ADC desonera a carga de trabalho dos servidores internos além de otimizar o fluxo de requisições, proporcionando uma maior economicidade tanto em termos financeiros quanto em termos de recursos computacionais.

d) Adicionalmente, a JF3R é participe em ata de registro de preço que está em andamento pelo Tribunal Regional Federal da 2ª Região - TRF2 para aquisição de licenças para o ambiente de virtualização de servidores, VMWare, que abrangerá funções de segurança de rede como Firewall e Balanceamento de carga em quesito de contingência.

e) A JF3R atualmente conta com dois data centers ativos, um no edifício-sede do Tribunal Regional Federal da 3ª Região – TRF3 e outro no edifício do Fórum Cível Ministro Pedro Lessa. Por ser uma solução em cluster, é necessário adquirir dois equipamentos por localidade, porém a Secretaria de Tecnologia da Informação - SETI desta corte almeja a contratação de um terceiro data center para aumentar a disponibilidade dos dados atuando como site de contingência. Assim, totalizando o quantitativo almejado necessário para o pleno funcionamento da ferramenta.

2.1.2.2 Da Justificativa de Padronização de Marca

a) Para isso, a JF3R pretende participar do Edital de Ata de Registro de Preços do Conselho da Justiça Federal (CJF), que visa à contratação de uma solução de Controlador de Entrega de Aplicações (ADC) da marca F5, modelo BIG-IP R4800. A escolha da referida solução pelo CJF tem como base a necessidade de padronização tecnológica com o Superior Tribunal de Justiça (STJ), órgão com o qual compartilha serviços e recursos de TI. O CJF e o STJ possuem uma infraestrutura tecnológica interligada, o que torna essencial a adoção de uma solução uniformizada para garantir compatibilidade, interoperabilidade e eficiência operacional.

b) Nesse norte, a manifestação de previsão da contratação da solução de Application Delivery Controller – ADC, fabricante F5, Modelo BIG-IP R4800, por parte da JF3R, tem fulcro nas alíneas a) e b) do inciso I do art. 41 da Lei 14.133/2021, como se pode observar:

"Art. 41. No caso de licitação que envolva o fornecimento de bens, a Administração poderá excepcionalmente:

I - indicar uma ou mais marcas ou modelos, desde que formalmente justificado, nas seguintes hipóteses:

a) em decorrência da necessidade de padronização do objeto;

b) em decorrência da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração;"

2.1.2.3 Das justificativas de necessidade de padronização, conforme alínea a) do inciso I do art. 41 da Lei 14.133/2021)

a) Objetivando participar do processo de estabelecimento de um padrão de maturidade unificado de segurança cibernética no âmbito da justiça federal (inciso III do Art. 12 da Resolução Nº 396 de 07/06/2021), a Divisão de Infraestrutura e Conectividade – DINC do Tribunal Regional Federal da 3ª Região entende que a adoção padronizada de soluções tecnológicas é uma estratégia fundamental para garantir as ações de fortalecimento da governança cibernética (inciso I do Art. 9 da Resolução Nº 396 de 07/06/2021), além de estar aderente ao disposto no art. 35 da Resolução Nº 370 de 28/01/2021, que versa sobre a recomendação de: "utilizar serviços em nuvem que simplificam a estrutura física, viabilizam a integração, requisitos aceitáveis de segurança da informação, proteção de dados, disponibilidade e padronização do uso dessa tecnologia no Poder Judiciário".

b) Apoiados na recomendação de utilização de serviços em nuvem, disposta no art. 35 da Resolução Nº 370 de

28/01/2021, ressalta-se o papel fundamental da Nuvem da Justiça Federal – NUJUFÉ no tocante às diretrizes de padronização de tecnologias, uma vez que, por se tratar de uma infraestrutura de nuvem compartilhada para processamento e disponibilização dos sistemas nacionais críticos da Justiça Federal, este ambiente precisa estar a apto a disponibilizar e proteger os sistemas de maneira uniforme e consolidada.

c) Considerando que cada Tribunal Regional Federal colabora em conjunto com o CJF no desenvolvimento e proteção dos sistemas nacionais hospedados e processados na NUJUFÉ (resolução n. 716/2021), é extremamente vantajoso do ponto de vista técnico, que as funcionalidades necessárias para publicação e proteção inerentes a solução de ADC sejam operacionalizadas de maneira padronizada e coordenada pela mesma solução adotada pelo CJF, órgão de cunho superior e responsável por exercer a coordenação central e padronização de procedimentos relativos a Tecnologia da Informação no âmbito da Justiça Federal.

d) Tendo em vista que este tribunal passará a utilizar módulo do Sistema Eletrônico de Recursos Humanos (SERH) no ambiente da Nuvem da Justiça Federal (NUJUFÉ) hospedada pelo CJF, e que este sistema precisará realizar transações de aplicações do tipo web entre os servidores de aplicação do CJF e da JF3R, é extremamente vantajoso do ponto de vista operacional e de cibersegurança, que os mecanismos de firewall de aplicação web e proteção contra ataques de negação de serviço desta aplicação e das futuras implementações de sistemas de cunho nacional sejam do mesmo fabricante do CJF.

e) É importante frisar que falta de padronização gera lacunas operacionais significativas, uma vez que soluções que não possuem capacidades de interoperabilidade limitam a capacidade de atuação coordenada entre os entes da Justiça Federal. Outro aspecto importante a considerar é a eficiência operacional. Com ferramentas padronizadas, as equipes de tecnologia da informação e segurança da informação da JF3R podem concentrar seus esforços em uma plataforma adotada previamente pela Justiça Federal, reduzindo a necessidade de treinamentos diversificados e suporte técnico para múltiplas soluções. Isso economiza tempo e recursos, além de melhorar a capacidade de resposta a incidentes, pois todos os membros das equipes de JF3R estarão familiarizados à mesma solução utilizada pelo CJF.

f) Do ponto de vista técnico, a escolha de uma solução padronizada de Application Delivery Controller (ADC) traz vantagens significativas que trazem eficiência operacional a este tribunal:

f.1) A possibilidade de intercâmbio de políticas, regras e configurações: Quando se utiliza uma única solução, as políticas de segurança e de entrega de aplicações podem ser facilmente replicadas e ajustadas em diferentes ambientes, permitindo uma implementação consistente e eficiente. Essa uniformidade é crucial para acelerar o processo de publicação e proteção dos sistemas, especialmente nos ambientes relacionados a sistemas nacionais da Justiça Federal, onde a consistência nas regras de segurança é um requisito fundamental.

f.2) Situações de disaster recovery: uma solução padronizada facilita a recuperação de instâncias do ADC. Se uma falha ocorrer em qualquer membro utilizador da solução de ADC padronizada, as equipes de TI da Justiça Federal podem rapidamente restaurar as configurações e políticas em um novo ambiente usando backups ou snapshots. Isso minimiza o tempo de inatividade e garante que as operações críticas possam ser retomadas com agilidade, mantendo a continuidade dos negócios.

f.3) Contribuição Técnico-Operacional: a adoção de uma solução única entre o STJ, CJF e os Tribunais Regionais Federais contribui para integração e o compartilhamento de experiências e informações relacionadas a tecnologia, possibilitando a convergência de esforços e iniciativas na apuração de incidentes e na promoção de ações de capacitação e educação em segurança cibernética.

g) Em suma, a padronização, o intercâmbio de políticas e a agilidade na recuperação são aspectos que não podem ser subestimados em um ecossistema de TI cada vez mais complexo e dinâmico.

h) Das justificativas de necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração, conforme a alínea b) do inciso I do art. 41 da Lei 14.133/2021).

i) Com relação a necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração, a adoção da solução de ADC padronizada permitirá que a JF3R esteja compatível com a solução a ser adquiridas pelo CJF, e já adquiridas por TRF1, STJ e por outros membros da Justiça Federal, possibilitando que operem os mecanismos de publicação e proteção de aplicações web (WAF) de maneira padronizada, aumentando a assertividade na resposta aos constantes ataques aos sistemas, o que é crucial para a proteção de sistemas críticos da Justiça Federal.

j) A adesão da JF3R à Ata de Registro de Preços do CJF justifica-se pela necessidade de compatibilidade com plataformas e padrões já adotados pela Administração, conforme previsto no artigo 41, inciso I, alínea "b" da Lei nº 14.133/21. O CJF e o STJ compartilham serviços e infraestrutura de TI, o que demanda soluções tecnológicas compatíveis para garantir a continuidade operacional e a segurança dos sistemas. A adoção do F5 BIG-IP R4800 como padrão pelo STJ e agora pelo CJF estabelece um ambiente homogêneo que facilita a integração entre os órgãos, reduz custos operacionais e minimiza riscos de incompatibilidade. Além disso, o uso de uma solução consolidada simplifica o gerenciamento da segurança cibernética, permitindo uma resposta mais eficiente a incidentes e ameaças digitais. Dessa forma, a escolha da JF3R em participar do Edital de ARP do CJF se alinha à necessidade de manter a compatibilidade tecnológica dentro do ecossistema da Justiça Federal, garantindo maior eficiência e confiabilidade nos serviços prestados.

2.1.2.4 Das Justificativas técnicas

a) Interoperabilidade e Integração de Serviços

a.1) Um ADC padronizado permite a uniformização das políticas de tráfego de rede e segurança, facilitando a administração conjunta dos serviços.

a.2) Garante conectividade eficiente e estável entre os sistemas das três instituições, evitando latência e incompatibilidades.

b) Segurança Cibernética Unificada

b.1) Permite a implementação centralizada de políticas de segurança, reduzindo vulnerabilidades e garantindo proteção uniforme contra ameaças cibernéticas.

b.2) O F5 BIG-IP R4800 possui WAF (Web Application Firewall) avançado, protegendo aplicações web contra ataques como DDoS, SQL Injection e Cross-Site Scripting (XSS).

b.3) Facilita a gestão de certificados SSL/TLS, assegurando criptografia padronizada em todas as comunicações entre os tribunais.

c) Continuidade e Alta Disponibilidade

c.1) A padronização permite configuração e gerenciamento integrados dos sites principais e de contingência, garantindo alta disponibilidade dos serviços judiciais

c.2) O modelo F5 BIG-IP R4800 permite balanceamento de carga inteligente, distribuindo requisições entre servidores para evitar sobrecarga e falhas.

c.3) Facilita a implementação de Disaster Recovery, garantindo que, em caso de falha em um tribunal, outro possa assumir a carga de trabalho sem interrupções.

d) Economia de Escala e Redução de Custos Operacionais - A adoção de uma única solução reduz custos de licenciamento, manutenção e suporte, pois permite contratação conjunta de serviços especializados.

d.1) Facilita a capacitação técnica da equipe de TI, pois o conhecimento adquirido sobre o ADC será comum entre os três órgãos, reduzindo a necessidade de treinamentos diferenciados.

d.2) Permite a compra de hardware e licenças em maior volume, possibilitando melhores condições comerciais. e) Eficiência Operacional e Gerenciamento Unificado

d.3) Um ADC padronizado possibilita gestão centralizada das regras de tráfego, políticas de segurança e desempenho das aplicações, tornando a administração mais eficiente.

d.4) O modelo F5 BIG-IP R4800 inclui ferramentas de automação e monitoramento, otimizando a visibilidade e resposta a incidentes. - Facilita a adoção de novas tecnologias e integrações futuras, evitando dificuldades de compatibilidade com soluções diversas.

e) A padronização da solução F5 BIG-IP R4800 no STJ, CJF e JF3R trará benefícios diretos em segurança, interoperabilidade, continuidade dos serviços e economia de escala, garantindo uma infraestrutura de TI robusta, eficiente e resiliente para a Justiça Federal.

2.1.2.5 Benefícios da Adoção da Solução Padronizada

a) A participação da JF3R na Ata de Registro de Preços do CJF para aquisição da solução F5 BIG-IP R4800 resultará em:

a.1) Maior integração e eficiência operacional com os tribunais superiores; - Redução de custos de suporte e manutenção ao adotar um padrão consolidado;

a.2) Facilidade na troca de informações e serviços entre CJF, STJ e JF3R; - Aprimoramento da segurança cibernética, garantindo resiliência contra ataques

a.3) Adoção de boas práticas e tecnologias já testadas e aprovadas pelo STJ e CJF.

b) Dessa forma, a participação da JF3R no Edital de ARP do CJF é justificada tanto pela necessidade de padronização quanto pela compatibilidade com padrões já adotados na Justiça Federal, em conformidade com o artigo 41, inciso I, alíneas "a" e "b" da Lei nº 14.133/21.

c) Ademais, indo ao encontro com a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) e com a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituídas pelo Conselho Nacional de Justiça – CNJ por meio das Resoluções n. 370/2021 e n. 396/2021, respectivamente, a presente contratação visa aumentar a satisfação dos usuários do sistema judiciário, promover serviços de infraestrutura e soluções corporativas além de aprimorar o nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário, a fim de alcançar um ambiente digital mais seguro e resiliente contra ameaças cibernéticas.

2.1.3 Motivação por parte do TRF5

2.1.3.1 Os seguintes fatores motivaram essa contratação:

- a) Reforço da segurança cibernética do TRF5 e Seções Judiciárias;
- b) Aumento da quantidade de ataques maliciosos às aplicações oferecidas pelo TRF5 e Seções Judiciárias;
- c) Aumento nos sistemas informatizados e processos digitais;
- d) Distribuição de tráfego para otimização do acesso aos serviços oferecidos.

2.1.3.2 Alinhamento Estratégico

2.1.3.2.1 O elevado grau de automação dos processos operacionais e administrativos leva as Organizações a confiar e depender cada vez mais de sua infraestrutura tecnológica para viabilizar aplicações de missão crítica e implementar rapidamente novas soluções que aumentem a agilidade, a capacidade de adaptação, a otimização de custos e a melhoria dos serviços prestados, de forma continuada, aos seus clientes e usuários. Atender a essa demanda por alta qualidade e eficiência com economia, confiabilidade, flexibilidade, agilidade e racionalização de fluxos de trabalho, é preocupação constante da alta direção dos órgãos, o que tornou a Tecnologia da Informação e Comunicação ferramenta estratégica que deve estar alinhada com as áreas de negócios da Instituição.

2.1.3.2.2 O serviço objeto de contratação encontra-se alinhado com o Plano Diretor de TI do TRF5ª Região através do objetivo estratégico "assegurar atuação sistêmica da TI na Justiça Federal"; bem como está contemplado na Iniciativa PDTI I.16 (Manutenção e Evolução de Soluções de Segurança da Informação) e compõe rol de ações vinculadas à estratégia de infraestrutura e segurança de TI do ciclo 2024-2026.

2.1.3.2.3 Face ao exposto e em conformidade com os princípios constitucionais de legalidade, impessoalidade, moralidade, publicidade e, em especial, de eficiência, a solução para o suporte aos usuários e às operações de TI descrita neste termo de referência e seus anexos constitui-se em objeto de contratação estratégico para o alcance das metas e propósitos perseguidos pela Justiça Federal.

2.1.3.3 Justificativa da Solução Escolhida

2.1.3.3.1 Cenário 01 – Não adquirir nenhuma solução.

a) Não é recomendável devido ao aumento exponencial de ataques maliciosos direcionados às aplicações. Um reforço na segurança cibernética é extremamente indicado, além da otimização do acesso aos serviços, cada vez ampliados e demandados.

2.1.3.3.2 Cenário 02 – Utilizar solução gratuita.

a) Não é recomendável devido, entre outras coisas, a demora na atualização de vacinas para bloqueio de tentativas de invasão e falta de suporte a apoio de fabricante.

2.1.3.3.3 Cenário 03 – Realizar licitação para adquirir solução moderna e eficiente.

a) Obviamente, por ser uma solução nova, há de se considerar os custos com treinamento, instalação, configuração e banco de horas de suporte, além de todo um processo exaustivo de migração.

2.1.3.3.4 Cenário 04 – Renovação da Solução de WAF atual

a) Trata-se de atender a dois projetos necessários: proteção do ambiente com WAF e Balanceamento de Carga. Por ser a solução atual do fabricante F5, de excelente qualidade, com ambas as funcionalidades pretendidas, já implantada e boa parte da equipe com experiência e capacitada. Mostra-se, do ponto de vista técnico, a mais adequada.

b) Há também de se considerar a mudança de perfil de acessos na JF5. Com a centralização dos sistemas nos sites do TRF5, JFPE e JFCE, será necessário a ampliação da capacidade da solução desses sites, permanecendo igual para os sites restantes. Assim, os primeiros serão ampliados para 10 GB de *throughput* e os outros continuam em 1 GB. Lembrando que a solução visa crescimento para 5 anos.

c) Por fim, conforme já comentado, a solução virtual já está ativa, estável e consolidada em toda 5ª Região. O projeto da JF5 visa implantar, gradualmente, a função de ADC, mas, primordialmente, manter e ampliar a utilização de Firewall de Ampliação. Em conversa com o fabricante, não houve objeções técnicas para a contratação dessa forma, principalmente pela situação atual já estabilizada e como será ativado o ADC, de forma gradual, ao longo dos próximos anos.

d) Em resumo:

d.1) Solução já implantada e estável, bastando apenas ser ampliada através de licenciamento, com ativação gradual de Balanceamento de Tráfego conforme projetos futuros;

d.2) Existências de recursos de virtualização disponíveis a fim de providenciar o necessário, garantindo economicidade e permanência da antiga contratação;

d.3) Conhecimento técnico da solução já incorporado à boa parte do corpo de servidores.

2.1.3.4 Quantitativo e Dimensionamento

2.1.3.4.1 Itens 2.1 e 2.2 - A Justiça Federal da 5ª Região é composta pelo TRF5, JFPE, JFCE, JFRN, JFAL, JFSE e JFPB. Cada um dos sites, atualmente, possui dois appliances virtuais, já funcionais há mais de 3 anos, exercendo a função de WAF (Web Application Firewall), trabalhando de forma ativo-passivo, de modo a garantir alta disponibilidade em caso de falha em uma das caixas. Eles foram dimensionados de acordo com o tráfego de dados de cada unidade na época: TRF5, JFPE e JFCE com throughput de 3 Gbps e JFRN, JFAL, JFSE e JFPB com 1 Gbps, para funcionamento apenas com a função de Firewall de Aplicação.

2.1.3.4.2 Nos próximos anos, haverá uma maior concentração de serviços nos sites maiores, deixando os outros sites basicamente com serviços locais.

2.1.3.4.3 Ainda, há o projeto de ativação da função de ADC para toda a região.

2.1.3.4.4 Links de Internet atuais (sites maiores): 2 x 5 Gbps para o TRF5, por exemplo, com previsão de crescimento ao longo dos próximos anos.

2.1.3.4.5 Links de Internet atuais (sites menores): 2 x 500 mbps para a JFPB, por exemplo, com previsão de baixo crescimento ao longo dos próximos anos.

2.1.3.4.6 Com essas premissas, concluímos:

a) Necessidade de aumento da capacidade dos appliances virtuais do TRF5, JFPE e JFCE devido a ativação gradual, ao longo dos próximos anos, da função de ADC e, também, devido a concentração de serviços da região nesses sites, além da manutenção e ampliação do serviço de WAF, já ativado.

b) Necessidade de aumento da capacidade dos *appliances* da JFRN, JFSE, JFAL, JFPB em contrapartida com sua necessidade redução, devido à migração dos serviços, implicando, assim, sua permanência com mesmo dimensionamento.

2.1.3.4.7 Item 2.3 – serviço de instalação: 1(um) serviço de instalação para cada *appliance* virtual;

2.1.3.4.8 Item 2.4 – suporte técnico por 12 meses, podendo ser renovado anualmente;

2.1.3.4.9 Item 2.5 – treinamento: 3 servidores por site.

2.1.3.4.10 Item 2.6 – 200 horas anuais para cada site, com a premissa da possibilidade de renovação a cada ano.

2.1.4 Motivação por parte do TRF6

2.1.4.1 Destaca-se que a solução de ADC objeto da presente contratação inclui recursos de balanceamento de links que não estão disponíveis na versão virtual em aquisição, razão pela qual é possível através do recurso dividir os acessos entre os IPs do TRF6. Considerando a recente sinalização positiva do STF para a cessão de um bloco de IPv4 /24, nos termos do Ofício STF Nº 2838011/STI (1149882), a disponibilidade do recurso de balanceamento permitirá ao TRF6 controlar os acessos aos seus sistemas, evitando, assim, eventuais sobrecargas.

2.1.4.2 Outra vantagem decorrente da contratação compartilhada decorre do modelo previsto, já que se trata do mesmo fabricante (F5) da solução vencedora do certame da aquisição de solução de segurança conduzida pelo TRF6, portanto em consonância com o Art. 41, I, b) da Lei n. 14.133/2021. Garante-se, assim, a total integração das soluções e, ainda, a administração única das regras, de forma a otimizar a atuação da equipe de segurança.

2.1.4.3 Deve-se destacar, ainda, um elemento essencial à infraestrutura: a disponibilidade. Todos os sistemas do TRF6 devem estar disponíveis para funcionamento em regime de 24 x 7 (vinte e quatro horas, sete dias por semana), o que pode acarretar em situações de falhas em horários sem acompanhamento por equipe especializada e, consequentemente, em atraso para o início do atendimento. Considerando que os sistemas e serviços de TI do TRF6 sustentam a área finalística da instituição, torna-se cada vez mais importante que estejam hospedados em ambiente de infraestrutura tecnológica protegida e que garanta a disponibilidade e integridade das informações.

2.1.4.4 A contratação visa a adquirir uma solução de segurança de alta complexidade diante da necessidade de implantação aderente à LGDP, em substituição ao atual sistema obsoleto de proteção de perímetro de rede com a inclusão de novas funcionalidades de proteção de rede que compõem a plataforma de segurança de nova geração. A nova solução incluirá recursos de balanceamento das aplicações e dos IPs de acesso, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões, sistemas de detecção de invasão e sistemas de prevenção de intrusão, aplicações antimalware, inspeção de pacotes SSL/TLS, já que o tráfego é frequentemente criptografado para evitar a detecção e bloqueio de ameaças. Também permitirá o combate à falsificação de tráfego de acesso, o que dificulta a identificação e o bloqueio com base em assinaturas ou padrões específicos em razão do caráter aparentemente legítimo, ao parque tecnológico do TRF6.

2.1.4.5 Por tudo exposto, busca-se com a presente contratação:

a) Atualizar o parque tecnológico do TRF6;

b) Obter serviços de alta disponibilidade;

- c) Aumentar a velocidade de operação entre os equipamentos;
- d) Otimizar o desempenho da rede de dados;
- e) Garantir a estabilidade operacional das comunicações do TRF6 e suas subseções judiciárias;
- f) Aumentar a proteção de rede do TRF6, possibilitando a inspeção de tráfego com maior granularidade que a atualmente realizada;
- g) Melhorar o desempenho e eficácia no controle de acesso ao perímetro de rede através de equipamentos com níveis de processamento e capacidade mais adequados;
- h) Distribuir uniformemente os acessos às aplicações entre os IPs reservados;
- i) Aumentar a disponibilidade das aplicações, evitando o comprometimento da capacidade do firewall em eventuais situações de ataque;
- j) Possuir viabilidade para realizar futuras expansões da capacidade e granularidade da rede do Tribunal;
- k) Possibilitar a ampliação da segmentação da rede com o objetivo de reduzir os riscos de segurança;
- l) Aumento da resiliência em caso de ataques;
- m) Diminuir o tempo de análise e resolução de problemas.

2.2. Objetivos a serem alcançados

2.2.1 Objetivos do CJF

2.2.1.1 São resultados esperados em decorrência da presente contratação:

- a) Garantir integridade, confidencialidade, autenticidade e disponibilidade das informações disponibilizadas pelos sistemas sustentados pela infraestrutura de tecnologia da informação do CJF;
- b) Proteger as aplicações sustentadas pelo CJF por meio de mecanismo de firewall de aplicação web (WAF), bloqueando e protegendo-as contra atividades maliciosas, tais como a manipulação do conteúdo exibido, injeções dos mais diversos tipos, proteção contra exploração de vulnerabilidades e invasões ao ambiente interno do órgão;
- c) Melhor experiência do usuário: redução no tempo de carregamento das páginas e melhoria na responsividade das aplicações;
- d) Maior disponibilidade: redução no tempo de inatividade das aplicações, garantindo acesso contínuo aos serviços *online*, mesmo em caso de queda do *data center* principal do CJF, localizado em seu edifício-sede;
- e) Segurança reforçada: proteção aprimorada contra ataques cibernéticos e vulnerabilidades de segurança.
- f) Eficiência operacional: melhor utilização dos recursos de servidores e redução de custos com infraestrutura.
- g) Escalabilidade: possibilitar que as aplicações sejam facilmente replicadas em termos quantitativos para atender ao aumento da demanda sem comprometer o desempenho.
- h) Flexibilidade: oferece flexibilidade para gerenciar e configurar o tráfego de aplicativos de acordo com as necessidades específicas do negócio.
- i) *Insights* de desempenho: obter análises e relatórios detalhados sobre o desempenho das aplicações, ajudando na tomada de decisões.

2.2.2 Objetivos do TRF3

2.2.2.1 Com a contratação em questão pretende-se alcançar os seguintes objetivos:

- a) Maior integração e eficiência operacional com os tribunais superiores;
- b) Redução de custos de suporte e manutenção ao adotar um padrão consolidado;
- c) Facilidade na troca de informações e serviços entre CJF, STJ e JF3R;
- d) Aprimoramento da segurança cibernética, garantindo resiliência contra ataques;
- e) Adoção de boas práticas e tecnologias já testadas e aprovadas pelo STJ e CJF.

2.2.3 Objetivos do TRF5

2.2.3.1 São resultados a serem alcançados pelo TRF5:

- a) Disponibilidade de sistemas e aplicações do TRF5 (PJe, PJe 2.0, Esparta, Portais, SGC, SEI, Diário Eletrônico, etc);
- b) Reforço da estrutura de Segurança da Informação, principalmente em virtude do aumento massivo de ataques cibernéticos à órgãos governamentais.
- c) Minimizar o risco de continuidade do negócio por ataques à infraestrutura de TI.
- d) Melhoria no nível de segurança de dados da Justiça Federal da 5ª Região;
- e) Melhoria de performance dos sistemas e serviços da 5ª Região

2.2.3.2 Conforme já comentado, a renovação das soluções de WAF atuais, que já possuem a função de ADC, facilitarão todo o processo de melhoria do ambiente, pois já estão implantadas com a funcionalidade de proteção, sendo expandidas para fornecer também ADC. Serão necessárias menos mudanças e adequações nos ambientes, causando menos impactos nos serviços fornecidos.

2.2.3.3 Por serem virtuais e já instaladas, será necessária apenas a aplicação do novo licenciamento, juntamente com a configuração do serviço de balanceamento.

2.2.4 Objetivos do TRF6

2.2.4.1 Busca-se com a presente contratação:

- a) Atualizar o parque tecnológico do TRF6;
- b) Obter serviços de alta disponibilidade;
- c) Aumentar a velocidade de operação entre os equipamentos;
- d) Otimizar o desempenho da rede de dados;
- e) Garantir a estabilidade operacional das comunicações do TRF6 e suas subseções judiciárias;
- f) Aumentar a proteção de rede do TRF6, possibilitando a inspeção de tráfego com maior granularidade que a atualmente realizada;
- g) Melhorar o desempenho e eficácia no controle de acesso ao perímetro de rede através de equipamentos com níveis de processamento e capacidade mais adequados;
- h) Distribuir uniformemente os acessos às aplicações entre os IPs reservados;
- i) Aumentar a disponibilidade das aplicações, evitando o comprometimento da capacidade do firewall em eventuais situações de ataque;
- j) Possuir viabilidade para realizar futuras expansões da capacidade e granularidade da rede do Tribunal;
- k) Possibilitar a ampliação da segmentação da rede com o objetivo de reduzir os riscos de segurança;
- l) Aumento da resiliência em caso de ataques;
- m) Diminuir o tempo de análise e resolução de problemas.

2.3. Alinhamento entre a contratação e o Plano Estratégico Institucional e/ou de TI e o Plano Anual de Contratações

2.3.1 A contratação está alinhada com as seguintes diretrizes estratégicas aplicáveis ao Conselho da Justiça Federal:

2.3.1.1 **Estratégia Nacional do Poder Judiciário 2021-2026** (*Resolução CNJ n. 325, de 30 de junho de 2020*):

2.3.1.1.1 Macrodesafio do Poder Judiciário:

- a) fortalecimento da estratégia nacional de TIC e de proteção de dados.

2.3.1.2 **Estratégia Nacional de Segurança da Informação do Poder Judiciário** (*Resolução CNJ n. 396, de 7 de junho de 2021*):

2.3.1.2.1 Objetivos estratégicos da ENSEC-PJ:

- a) tornar o Judiciário mais seguro e inclusivo no ambiente digital;
- b) aumentar a resiliência às ameaças cibernéticas;
- c) permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

2.3.1.3 **Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário 2021-2026** (*Resolução CNJ n. 370 de 28 de janeiro de 2021*):

2.3.1.3.1 Objetivos estratégicos da ENTIC-JUD:

- a) aprimorar a Segurança da Informação e a Gestão de Dados;
- b) promover Serviços de Infraestrutura e Soluções Corporativas.

2.3.1.4 Estratégia do Conselho da Justiça Federal (Portaria CJF n. 576, de 24 de junho de 2020):

2.3.1.4.1 Objetivo estratégico do CJF sob a perspectiva de Pessoas e Recursos:

- a) fortalecer a segurança da informação: promover ações que objetivam viabilizar e assegurar a disponibilidade, a integridade e a confidencialidade das informações, assim como a transparência e a proteção aos dados pessoais, desde a sua coleta até o seu processamento e o compartilhamento.

2.3.1.5 Plano Estratégico de Tecnologia da Informação da Justiça Federal (Resolução CJF n. 685, de 15 de dezembro de 2020):

2.3.1.5.1 Objetivos estratégicos do PETI:

- a) aperfeiçoar e assegurar a efetividade dos serviços de TI para a Justiça Federal;
- b) promover e fortalecer a segurança da informação digital na Justiça Federal.

2.3.1.6 Plano Diretor de TI – PDTI do CJF 2024-2026:

2.3.1.6.1 Iniciativas do Plano Diretor de TI:

- a) INIC-2024-003 - Aprimorar política e procedimentos de segurança da informação;
- b) INIC-2024-004 - Aperfeiçoar procedimentos de infraestrutura de TI;
- c) INIC-2024-006 - Aprimorar o fornecimento de serviços de TI para os usuários da Justiça Federal.

2.3.1.7 Plano de Contratações Anual CJF – 2024

1.4.1 A contratação está prevista no Plano de Contratações Anual – PCA 2025 do Conselho da Justiça Federal, item 153, processo SEI nº 0001092-21.2024.4.90.8000, bem como no item 12 do Plano de Contratações Compartilhadas Anual – PCCA 2025.

2.4. Referência aos Estudos Preliminares da Solução de TI

2.4.1 Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda – DOD (id. 0565535) e o Estudo Técnico Preliminar - ETP (id. 0698410) acostados ao processo SEI n. 0000919-34.2024.4.90.8000.

2.4.2 A presente instrução processual contemplou a formulação de estudo técnico preliminar no qual foi concluída a viabilidade da contratação ante à identificação da necessidade e análise da solução adequada do problema à luz do interesse público.

2.4.3 Identificou-se também, no referido estudo, os requisitos necessários à contratação, a estimativa de quantidades e do valor, a descrição da solução como um todo, os resultados pretendidos e as providências a serem adotadas pela Administração, dentre outros temas.

2.5. Relação entre a demanda prevista e a quantidade de bens e/ou serviços a serem contratados (Art. 18, § 1º, IV, Lei 14.133/2021)

2.5.1. Quantitativo relativo ao CJF

2.5.1.1 Segundo a arquitetura proposta (Anexo III), serão necessários 2 (dois) equipamentos ADC do fabricante F5, modelo BIG-IP R4800, para interconexão com os equipamentos já adquiridos pelo STJ, de forma a possibilitar a formação de dois *clusters* de entrega de aplicações e sítio de contingência nos *data centers* do CJF e do STJ, que estão separados geograficamente.

2.5.1.2 Ademais, também será contratado o serviço de instalação e configuração da solução, visto que se trata de tecnologia especializada com alto grau de complexidade, o qual deverá ser planejado junto à equipe técnica do CONTRATANTE e deverá ser realizado por profissionais devidamente certificados pelo fabricante da solução adquirida. Esse serviço será utilizado uma única vez no início da contratação para ambos os equipamentos.

2.5.1.3 O certificado do fabricante que comprove a qualificação do profissional para realização das atividades prevista deverá ser apresentado na data inicial da prestação do serviço.

2.5.1.4 Além disso, haverá a prestação de suporte técnico presencial, aferido mensalmente, durante toda vigência contratual, de forma a garantir o correto funcionamento da solução e o emprego eficiente de suas funcionalidades para atender às necessidades do CONTRATANTE.

2.5.1.5 Como se trata de tecnologia de ponta, também será contratada uma ação de Transferência de Conhecimento com

carga horária mínima de 40h, a ser ministrado para até 21 (vinte e um) servidores da STI, online e sob demanda, com pagamento realizado por aluno, ou seja, para cada servidor a ser treinado. Tendo em vista a alta rotatividade de pessoal da STI/CJF, a ação de Transferência de Conhecimento poderá ser demandada ao longo da vigência contratual.

2.5.1.6 Por fim, haverá o serviço técnico especializado para implementação e customização da solução, os quais estarão disponíveis durante toda a vigência contratual, mas somente serão utilizados sob demanda, sem garantia mínima de utilização. Esse serviço é de suma importância, visto que haverá a necessidade de migração de diversas configurações e regras da solução atual para a nova, além da possibilidade de se implementar funcionalidades disponíveis nos novos equipamentos que ainda não são utilizadas pelo CJF.

2.5.2. Quantitativo relativo ao TRF3

2.5.2.1 As justificativas quanto ao quantitativo a ser registrado pelo TRF3 estão contidas na redação do item 2.1.2 (Motivação por parte do TRF3).

2.5.3. Quantitativo relativo ao TRF5

2.5.3.1 As justificativas quanto ao quantitativo a ser registrado pelo TRF5 estão contidas na redação do item 2.1.3 (Motivação por parte do TRF5).

2.5.4. Quantitativo relativo ao TRF6

2.5.4.1 As justificativas quanto ao quantitativo a ser registrado pelo TRF6 estão contidas na redação do item 2.1.4 (Motivação por parte do TRF6).

2.6. Análise de mercado de Tecnologia da Informação e Comunicação com o levantamento das soluções disponíveis e/ou contratadas por órgãos ou entidades da Administração Pública, seus respectivos valores, bem como a definição e a justificativa da escolha da solução

2.6.1 A partir do Documento de Oficialização da Demanda – DOD (id. 0565535), foi realizado o Estudo Técnico Preliminar (id. 0698410), ocasião na qual foram levantados os requisitos técnicos e de negócio atrelados à necessidade do CJF e demais órgãos partícipes. Dentre as alternativas de soluções ADC existentes no mercado, analisou-se as seguintes:

- a) Solução ADC em nuvem, contratada como serviço, no modelo conhecido como ADCaaS (*ADC as a Service*);
- b) Solução ADC em *software* livre;
- c) Solução ADC física, no modelo *on-premise*;
- d) Solução ADC virtual, no modelo *on-premise*.

2.6.2 Assim, no contexto do CJF, TRF3 e TRF6, dentre as opções que atendem ao escopo pretendido e, ainda, levando-se em consideração os requisitos técnicos e de negócio, riscos, vantagens e desvantagens técnicas, a alternativa que se apresenta como adequada e viável nos termos fundamentados no Estudo Técnico Preliminar é a aquisição de solução ADC física, no modelo *on-premise*.

2.6.3 Registra-se que o TRF5, mediante justificativas técnicas apresentadas, escolheu a solução ADC virtual, no modelo *on-premise*, já que é o modelo atualmente utilizado por aquele Tribunal e ao qual pretende-se dar continuidade.

2.7. Custo total estimado para a contratação (Art. 6º, XXIII, "i", Lei n. 14.133/2021)

2.7.1 Para a realização da estimativa de custo da presente contratação, foram consultadas empresas especializadas no segmento de mercado, ocasião na qual foi enviado a descrição do objeto a ser contratado, bem como as especificações técnicas dos equipamentos a serem adquiridos. Contudo, tendo em vista que a solução a ser contratada é a mesma do STJ e que ela foi adquirida há apenas 6 (seis) meses antes da concretização dos estudos técnicos preliminares, decidiu-se por tomar como base o valor reajustado do Contrato STJ n. 108/2023, assinado em 11/12/2023.

2.7.2 Para o reajuste dos valores firmados no contrato do STJ, utilizou-se o seguinte:

- a) para o **item 1** do objeto (equipamentos ADC): variação do dólar no período; e
- b) para os **itens 2, 3 e 4** (serviços de instalação, configuração, suporte técnico e treinamento): Índice de Custo da Tecnologia da Informação – ICTI, disponibilizado pelo Instituto de Pesquisa Econômica Aplicada – IPEA.

2.7.3 Posteriormente, verificou-se que as cotações encaminhadas pelas empresas consultadas continham preços considerados excessivamente elevados, pois estavam pelo menos 30% mais caros que o valor reajustado do contrato do STJ. Portanto, foram desconsiderados.

2.7.4 Ainda, foram observadas as empresas licitantes que participaram do Pregão Eletrônico STJ n. 110/2023 e os seus lances iniciais e finais durante o certame. Com isso, restou confirmado que o valor reajustado do contrato do STJ é, de fato, exequível e está alinhado com o praticado pelo mercado.

2.7.5 Assim, o custo total médio estimado para a presente contratação, para o prazo de 60 (sessenta) meses é:

- Para o CJF: R\$ 6.557.629,61 (seis milhões, quinhentos e cinquenta e sete mil seiscentos e vinte e nove reais e sessenta e um centavos);
- Para o TRF3: R\$ 5.622.091,61 (cinco milhões, seiscentos e vinte e dois mil noventa e um reais e sessenta e um centavos);
- Para a SJSP: R\$ 5.311.151,61 (cinco milhões, trezentos e onze mil cento e cinquenta e um reais e sessenta e um centavos);
- Para a SJMS: R\$ 5.311.151,61 (cinco milhões, trezentos e onze mil cento e cinquenta e um reais e sessenta e um centavos);
- Para o TRF5: R\$ 2.479.086,98 (dois milhões, quatrocentos e setenta e nove mil oitenta e seis reais e noventa e oito centavos);
- Para a JFPE: R\$ 2.479.086,98 (dois milhões, quatrocentos e setenta e nove mil oitenta e seis reais e noventa e oito centavos);
- Para a JFCE: R\$ 2.479.086,98 (dois milhões, quatrocentos e setenta e nove mil oitenta e seis reais e noventa e oito centavos);
- Para a JFPB: R\$ 1.517.038,98 (um milhão, quinhentos e dezessete mil trinta e oito reais e noventa e oito centavos);
- Para a JFAL: R\$ 1.517.038,98 (um milhão, quinhentos e dezessete mil trinta e oito reais e noventa e oito centavos);
- Para a JFSE: R\$ 1.517.038,98 (um milhão, quinhentos e dezessete mil trinta e oito reais e noventa e oito centavos);
- Para a JFRN: R\$ 1.517.038,98 (um milhão, quinhentos e dezessete mil trinta e oito reais e noventa e oito centavos);
- Para o TRF6: R\$ 5.537.087,61 (cinco milhões, quinhentos e trinta e sete mil oitenta e sete reais e sessenta e um centavos).

Grupo	Item	Descrição	Unidade	CJF	
				Quantidade a ser contratada	Custo Médio Estimado
1	1.1	Appliance físico para solução de Application Delivery Controller – ADC, fabricante F5, Modelo BIG-IP R4800	Unidade	2	R\$ 4.252.199,65
	1.2	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 197.933,96
	1.3	Serviço de garantia e suporte técnico presencial para a solução ADC	Mês	60	R\$ 801.960,00
	1.4	Transferência de conhecimento online, com carga horária mínima de 40h	Pessoa	4	R\$ 124.376,00
	1.5	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	2400	R\$ 1.181.160,00
					R\$ 6.557.629,61

				TRF3
--	--	--	--	------

Grupo	Item	Descrição	Unidade	Quantidade	Custo Médio Estimado
1	1.1	Appliance físico para solução de Application Delivery Controller – ADC, fabricante F5, Modelo BIG-IP R4800	Unidade	2	R\$ 4.252.199,65
	1.2	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 197.933,96
	1.3	Serviço de garantia e suporte técnico presencial para a solução ADC	Mês	60	R\$ 801.960,00
	1.4	Transferência de conhecimento online, com carga horária mínima de 40h	Pessoa	10	R\$ 310.940,00
	1.5	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	120	R\$ 59.058,00
					R\$ 5.622.091,61

Grupo	Item	Descrição	Unidade	SJSP	
				Quantidade	Custo Médio Estimado
1	1.1	Appliance físico para solução de Application Delivery Controller – ADC, fabricante F5, Modelo BIG-IP R4800	Unidade	2	R\$ 4.252.199,65
	1.2	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 197.933,96
	1.3	Serviço de garantia e suporte técnico presencial para a solução ADC	Mês	60	R\$ 801.960,00
	1.4	Transferência de conhecimento online, com carga horária mínima de 40h	Pessoa	0	R\$ -
	1.5	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	120	R\$ 59.058,00
					R\$ 5.311.151,61

Grupo	Item	Descrição	Unidade	SJMS	
				Quantidade	Custo Médio Estimado
1	1.1	Appliance físico para solução de Application Delivery Controller – ADC, fabricante F5, Modelo BIG-IP R4800	Unidade	2	R\$ 4.252.199,65
	1.2	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 197.933,96
	1.3	Serviço de garantia e suporte técnico presencial para a solução ADC	Mês	60	R\$ 801.960,00
	1.4	Transferência de conhecimento online, com carga horária mínima de 40h	Pessoa	0	R\$ -
	1.5	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	120	R\$ 59.058,00
					R\$ 5.311.151,61

Grupo	Item	Descrição	Unidade	TRF5	
				Quantidade	Custo Médio Estimado
2	2.1	Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	0	R\$ -
	2.2	Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	2	R\$ 1.934.895,00
	2.3	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 91.384,14
	2.4	Serviço de suporte técnico remoto para a solução ADC	Mês	12	R\$ 256.644,00

	2.5	Transferência de conhecimento <i>online</i> , com carga horária mínima de 40h	Pessoa	3	R\$ 105.963,84
	2.6	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	200	R\$ 90.200,00
					R\$ 2.479.086,98

Grupo	Item	Descrição	Unidade	JFPE	
				Quantidade	Custo Médio Estimado
2	2.1	Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	0	R\$ -
	2.2	Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	2	R\$ 1.934.895,00
	2.3	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 91.384,14
	2.4	Serviço de suporte técnico remoto para a solução ADC	Mês	12	R\$ 256.644,00
	2.5	Transferência de conhecimento <i>online</i> , com carga horária mínima de 40h	Pessoa	3	R\$ 105.963,84
	2.6	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	200	R\$ 90.200,00
					R\$ 2.479.086,98

Grupo	Item	Descrição	Unidade	JFCE	
				Quantidade	Custo Médio Estimado
2	2.1	Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	0	R\$ -
	2.2	Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	2	R\$ 1.934.895,00
	2.3	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 91.384,14
	2.4	Serviço de suporte técnico remoto para a solução ADC	Mês	12	R\$ 256.644,00
	2.5	Transferência de conhecimento <i>online</i> , com carga horária mínima de 40h	Pessoa	3	R\$ 105.963,84
	2.6	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	200	R\$ 90.200,00
					R\$ 2.479.086,98

Grupo	Item	Descrição	Unidade	JFPB	
				Quantidade	Custo Médio Estimado

2	2.1	Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	2	R\$ 972.847,00
	2.2	Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	0	R\$ -
	2.3	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 91.384,14
	2.4	Serviço de suporte técnico remoto para a solução ADC	Mês	12	R\$ 256.644,00
	2.5	Transferência de conhecimento <i>online</i> , com carga horária mínima de 40h	Pessoa	3	R\$ 105.963,84
	2.6	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	200	R\$ 90.200,00
					R\$ 1.517.038,98

Grupo	Item	Descrição	Unidade	JFAL	
				Quantidade	Custo Médio Estimado

2	2.1	Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	2	R\$ 972.847,00
	2.2	Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	0	R\$ -
	2.3	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 91.384,14
	2.4	Serviço de suporte técnico remoto para a solução ADC	Mês	12	R\$ 256.644,00
	2.5	Transferência de conhecimento online, com carga horária mínima de 40h	Pessoa	3	R\$ 105.963,84
	2.6	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	200	R\$ 90.200,00
					R\$ 1.517.038,98

Grupo	Item	Descrição	Unidade	JFSE	
				Quantidade	Custo Médio Estimado
	2.1	Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	2	R\$ 972.847,00
	2.2	Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	0	R\$ -

2	2.3	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 91.384,14
	2.4	Serviço de suporte técnico remoto para a solução ADC	Mês	12	R\$ 256.644,00
	2.5	Transferência de conhecimento <i>online</i> , com carga horária mínima de 40h	Pessoa	3	R\$ 105.963,84
	2.6	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	200	R\$ 90.200,00
					R\$ 1.517.038,98

Grupo	Item	Descrição	Unidade	JFRN	
				Quantidade	Custo Médio Estimado
2	2.1	Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	2	R\$ 972.847,00
	2.2	Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	0	R\$ -
	2.3	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 91.384,14

	2.4	Serviço de suporte técnico remoto para a solução ADC	Mês	12	R\$ 256.644,00
	2.5	Transferência de conhecimento <i>online</i> , com carga horária mínima de 40h	Pessoa	3	R\$ 105.963,84
	2.6	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	200	R\$ 90.200,00
					R\$ 1.517.038,98

Grupo	Item	Descrição	Unidade	TRF6	
				Quantidade	Custo Médio Estimado
1	1.1	Appliance físico para solução de Application Delivery Controller – ADC, fabricante F5, Modelo BIG-IP R4800	Unidade	2	R\$ 4.252.199,65
	1.2	Serviço de instalação e configuração da solução ADC	Unidade	2	R\$ 197.933,96
	1.3	Serviço de garantia e suporte técnico presencial para a solução ADC	Mês	60	R\$ 801.960,00
	1.4	Transferência de conhecimento online, com carga horária mínima de 40h	Pessoa	6	R\$ 186.564,00
	1.5	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	200	R\$ 98.430,00
					R\$ 5.537.087,61

Grupo	Item	Descrição	Unidade	Quantidade Total CJF + TRFs	Custo Médio Unitário	Valor Médio Global estimado CJF+TRFS
1	1.1	Appliance físico para solução de Application Delivery Controller – ADC, fabricante F5, Modelo BIG-IP R4800	Unidade	10	R\$ 2.126.099,83	R\$ 21.260.998,26

	1.2	Serviço de instalação e configuração da solução ADC	Unidade	10	R\$ 98.966,98	R\$ 989.669,80
	1.3	Serviço de garantia e suporte técnico presencial para a solução ADC	Mês	300	R\$ 13.366,00	R\$ 4.009.800,00
	1.4	Transferência de conhecimento online, com carga horária mínima de 40h	Pessoa	20	R\$ 31.094,00	R\$ 621.880,00
	1.5	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	2960	R\$ 492,15	R\$ 1.456.764,00
2	2.1	Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	8	R\$ 486.423,50	R\$ 3.891.388,00
	2.2	Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses	Unidade	6	R\$ 967.447,50	R\$ 5.804.685,00
	2.3	Serviço de instalação e configuração da solução ADC	Unidade	14	R\$ 45.692,07	R\$ 639.688,98
	2.4	Serviço de suporte técnico remoto para a solução ADC	Mês	84	R\$ 21.387,00	R\$ 1.796.508,00
	2.5	Transferência de conhecimento <i>online</i> , com carga horária mínima de 40h	Pessoa	21	R\$ 35.321,28	R\$ 741.746,88
	2.6	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	1400	R\$ 451,00	R\$ 631.400,00
						R\$ 41.844.528,92

2.7.6 A análise detalhada da pesquisa de mercado e a memória de cálculo podem ser acessadas no ETP (id. 0698410, item 1.13) e no Mapa Comparativo de Preços (id. 0701697).

2.7.7 Desta forma, será adotado pelo CJF o seguinte índice de reajuste:

a) Para todos os itens dos Grupos 1 e 2: Índice de Custo da Tecnologia da Informação – ICTI, disponibilizado pelo Instituto de Pesquisa Econômica Aplicada – IPEA.

2.7.8 De forma a complementar a pesquisa de preços, foi realizada pesquisa de preços com fornecedores do mercado, pois há dificuldade em se encontrar preços públicos em decorrência do detalhamento do objeto deste Termo de Referência, não tendo sido possível localizar quantidade adequada de preços públicos para todos os itens.

2.8. Natureza do objeto a ser contratado (Art. 6º, XXIII, “a” da Lei 14.133/2021)

2.8.1 O objeto da presente contratação pode ser objetivamente especificado por meio de padrões usuais de mercado. Dessa forma, entende-se que esse objeto é classificado como bens e serviços comuns para fins do disposto no art. 6º, inciso XIII, da Lei n 14.133/2021, podendo, portanto, ser contratado por meio de processo licitatório na modalidade Pregão, preferencialmente na forma eletrônica.

2.8.2 Natureza do objeto:

2.8.2.1 Quanto à natureza do objeto, de acordo com o art. 2º da IN 12/2022 - CJF, os serviços são classificados, quanto a sua natureza, como de caráter contínuo:

“Art. 2º Consideram-se serviços e fornecimentos contínuos aqueles que, pela sua essencialidade, visam atender à necessidade pública de maneira permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público ou o

funcionamento das atividades do CJF, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional.”

2.9. Conformidade técnica e legal do objeto

2.9.1 O presente Termo de Referência foi elaborado em conformidade com as seguintes normas:

- a) Lei n. 14.133/2021, que regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos administrativos;
- b) Resolução CNJ n. 468/2022, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça;
- c) Portaria CJF n. 232/2023, que dispõe sobre as etapas do planejamento da contratação, para aquisição de bens e contratações de serviços sob o regime de execução indireta, no âmbito do Conselho da Justiça Federal;
- d) Resolução CJF n. 6/2008, alterada pela Resolução CJF n. 687, de 15 de dezembro de 2020, que dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2º graus;
- e) Portaria CNJ n. 162/2021, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

2.10. Justificativa para o parcelamento ou não da solução de TIC (Art. 18, § 1º, VIII, Lei n. 14.133/2021)

2.10.1 O objeto desta contratação será dividido em 2 (dois) grupos, cada um referente a um modelo de solução ADC:

- a) **GRUPO 1 (CJF, TRF3, JFSP, JFMS e TRF6)**: solução ADC física, no modelo *on-premise*, incluindo *appliances* físicos ADC e os serviços de instalação, configuração, suporte técnico mensal, transferência de conhecimento e serviços técnicos especializados para implementação e customização da solução;
- b) **GRUPO 2 (TRF5, JFPE, JFCE, JFPB, JFAL, JFSE e JFRN)**: solução ADC virtual, no modelo *on-premise*, incluindo *appliances* virtuais ADC e os serviços de instalação, configuração, suporte técnico mensal, transferência de conhecimento e serviços técnicos especializados para implementação e customização da solução.

2.10.2 Inicialmente, é de se destacar que, embora ambos os grupos que compõem o objeto da contratação em tela sejam relativos à solução ADC, há a necessidade de separação conforme suas características singulares em termos técnicos e de execução contratual. A saber, o GRUPO 1 trata de solução ADC constituída por *appliances* físicos e prestação de suporte técnico presencial por 60 (sessenta) meses. Já o GRUPO 2 trata de solução ADC constituída por 2 (dois) tipos de *appliance* virtual e serviço de suporte técnico, prestado de maneira remota, pelo prazo de 12 (doze) meses.

2.10.3 Embora o objeto de uma contratação deva ser majoritariamente parcelado, os itens que compõem cada grupo da presente aquisição não o serão, uma vez que os componentes os quais integram o objeto formam um conjunto indissociável e integrados para o perfeito funcionamento da solução almejada. Ademais, os itens de cada grupo apresentam inter-relação entre si, de forma que assegurem o alinhamento e a coerência em termos de qualidade técnica, resultando assim, no perfeito atendimento dos princípios da celeridade, economicidade e eficiência almejados na contratação.

2.10.4 Somente a execução de forma integrada dos componentes e dos serviços garante a qualidade das entregas, evitando transferência de responsabilidades, o que pode não ocorrer caso a prestação de serviço de cada grupo seja prestado por empresas diferentes. Ou seja, o parcelamento do objeto de cada grupo seria prejudicial do ponto de vista técnico-administrativo.

2.10.5 Para se garantir a viabilidade técnico-administrativa desta contratação, é fundamental que todos os itens a serem contratados de um mesmo grupo, incluindo *appliances* físico/virtuais e serviços decorrentes de instalação, configuração, suporte técnico mensal, transferência de conhecimento e customização sob demanda, sejam todos adjudicados para um único licitante vencedor, pois o objeto configura um sistema único, indissolúvel e integrado, conforme versa o art. 40, § 3º, II, da Lei n. 14.133/2021. Caso as responsabilidades da solução sejam divididas entre mais de uma empresa contratada, o CJF se exporá a riscos relativos a falhas de integração, de não completude da solução e de aumento exacerbado da complexidade em se gerir e fiscalizar as responsabilidades entre diversas empresas.

2.10.6 A orientação do TCU no Acórdão nº 861/2013 – Plenário é a seguinte: "São lícitos os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si". Portanto, é admitida a possibilidade do agrupamento de itens em lote único nos pregões eletrônicos.

2.10.7 Assim, para que se garanta a compatibilidade técnica do conjunto da solução, bem como uma maior eficiência e racionalidade administrativa, o agrupamento de todos os itens que compõem a solução configura-se como a melhor alternativa para os CONTRATANTES.

2.11. Permissão consórcio, cooperativa e/ou subcontratação da solução de TIC, justificando-se a decisão (Arts. 15 e

2.11.1 É vedada a participação de empresas em consórcio ou a subcontratação da solução, pois não há questões de alta complexidade e de relevante vulto, que impeçam a participação isolada de empresas e assim justificar a união de esforços.

2.11.2 Neste tipo de objeto, a participação em consórcio não amplia o leque de concorrentes, apenas aumenta a complexidade administrativa da gestão contratual.

3. Forma e critério de seleção de fornecedor (Art. 6º, XXIII, "h", Lei n. 14.133/2021)

3.1. Modalidade e critério de julgamento (Arts. 28 e 33, Lei n. 14.133/2021)

3.1.1 Classifica-se o serviço a ser fornecido como comum, conforme Acórdão 2.471/2008-TCU-Plenário, assim definida a forma de seleção do fornecedor como LICITAÇÃO, na modalidade PREGÃO, com o critério de julgamento MENOR PREÇO POR GRUPO, a ser realizada por meio de registro de preços, como determina o Art. 15 da Resolução-CJF 842/2023, com vistas a obter a melhor proposta para a Administração Pública, em observância ao Art. 33 da Lei n. 14.133/2021.

3.1.2 Os preços serão finais e definitivos e neles deverão estar inclusos todos os encargos fiscais e comerciais resultantes da contratação. Os valores máximos aceitos pela Administração para aquisição serão os valores constantes das propostas ofertadas pelas empresas.

3.2. Fundamentação legal do sistema de registro de preços (Decreto n. 11.462, de 31 de março de 2023)

3.2.1. O Sistema de Registro de Preços – SRP, regulamentado pelo Decreto n. 11.462, de 31 de março de 2023, prevê em seu art. 3º, inciso III, que o SRP poderá ser adotado nas seguintes hipóteses:

a) quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas;

3.2.2. Considerando que a referida contratação seria realizada de forma compartilhada, juntamente com os TRFs da 3ª, 5ª e 6ª regiões, foi sugerida a adoção do Sistema de Registro de Preços – SRP;

3.2.3. Ante o exposto, a presente contratação enquadra-se na hipótese do inciso supracitado, sendo conveniente e adequada a adoção do SRP para realizar contratações para atendimento aos órgãos participantes desta contratação;

3.2.4 O Conselho da Justiça Federal será o órgão gestor da Ata de Registro de Preços;

3.2.5. Conforme art. 86 da Lei n. 14.133, o CJF deverá, na fase preparatória do processo licitatório, para fins de registro de preços, realizar procedimento público de divulgação da Intenção de Registro de Preços (IRP), porém considerando que os órgãos da Justiça Federal foram consultados, que a contratação será conjunta com os órgãos da Justiça Federal que manifestaram interesse e está prevista a possibilidade de outros órgãos da Justiça Federal aderirem à Ata de Registro de Preço posteriormente, considerando o art. 25-E da Resolução CJF N. 842/2023, este Conselho poderá dispensar a publicação da Intenção de Registro de Preços, posto que não dispõe de capacidade de gerenciamento adicional de novos participantes.

3.2.6 Para a presente seleção, as licitantes não podem oferecer propostas em quantitativo inferior ao máximo previsto no edital, nos termos do inc. IV do art. 82 da Lei n. 14.133, de abril de 2021;

3.2.7 Não serão permitidas adesões posteriores, salvo a possibilidade de adesão à Ata de Registro de Preços por parte dos órgãos da Justiça Federal, conforme art. 30 da Resolução CJF n. 842/2023 (0509668), bem como dos órgãos descritos no Termo de Cooperação Técnica CNJ n. 16/2024 (0656269), enquanto não participantes, no formato conhecido como "carona".

3.2.8 Não serão aceitas propostas com preços diferenciados em razão do local de entrega do objeto.

3.3. Critérios de seleção do fornecedor (Art. 6º, XXIII, "h", Lei n. 14.133/2021)

3.3.1. O licitante que apresentar documentação de habilitação em desacordo com o Edital desta contratação será inabilitado;

3.3.2. Quando da formulação de sua proposta, a licitante deverá especificar de forma clara, completa e minuciosa, todos os bens e serviços ofertados, conforme os itens que compõem o Grupo do objeto ao qual está concorrendo;

3.3.3. Observar, quando da formulação de sua proposta, as especificações e características obrigatórias, não sendo permitida a oferta de preços alternativos ou a inclusão de condições que impeçam o julgamento objetivo da licitação;

3.3.4. A proposta deverá indicar em qual página e item da documentação está a comprovação do atendimento aos requisitos técnicos descritos nos Anexos I e II, de acordo com Grupo do objeto a que se referem, conforme a seguir:

a) Grupo 1 (solução ADC física): Anexo I;

b) Grupo 2 (solução ADC virtual): Anexo II.

3.3.5. O CJF poderá diligenciar com a licitante, caso a proposta não indique a página e item conforme exigido, sem que isso implique a desclassificação imediata da proposta apresentada;

3.3.6. A proposta deverá incluir, em versão eletrônica, todos os catálogos ou prospectos do fabricante (ou link para recursos que possam ser acessados pela Internet), preferencialmente em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), correspondente aos produtos descritos nos Anexos I e II deste Termo de Referência, com descrição detalhada de cada item;

3.3.7. O valor total de cada item não poderá ser superior ao valor estimado no Edital, mesmo a licitante tendo proposto o menor preço global por grupo;

3.3.8. A licitante deverá apresentar comprovação aos critérios de sustentabilidade, conforme previsto no item 4.14 deste Termo.

3.3.9 A licitante deverá apresentar, até o momento da assinatura do Contrato, declaração emitida pelo fabricante, informando estar apta e autorizada a comercializar os produtos e/ou serviços objeto da licitação ou ter registro no site do fabricante.

3.3.10. Critérios técnicos

3.3.10.1. Respeitado o disposto no art. 67, §1º e §2º da Lei n. 14.133/2021, as empresas licitantes deverão apresentar atestado(s) de capacidade técnica, emitido(s) por pessoas jurídicas de direito público ou privado, para os Grupos 1 e 2 do objeto deste certame, conforme detalhado a seguir:

3.3.10.1.1. Para o GRUPO 1:

- a) Fornecimento de 3 (três) *appliances* físicos para solução ADC, de características iguais ou similares ao modelo especificado no ANEXO I;
- b) Instalação e configuração de solução ADC física, no modelo *on-premise*, composta por, no mínimo, 1 (um) *appliance*;
- c) Prestação de suporte técnico presencial para solução ADC física, instalada no modelo *on-premise*, pelo durante toda a vigência contratual.

3.3.10.1.2. Para o GRUPO 2:

- a) Fornecimento de 4 (quatro) *appliances* virtuais para solução ADC, incluindo os seus respectivos licenciamentos/subscrições, de características iguais ou similares aos modelos especificados no ANEXO II;
- b) Instalação e configuração de solução ADC virtual, no modelo *on-premise*, composta por, no mínimo, 2 (dois) *appliances*;
- c) Prestação de suporte técnico, remoto, para solução ADC (física ou virtual), instalada no modelo *on-premise*, durante toda a vigência contratual.

3.3.10.2. Será aceito o somatório de atestados para comprovação da capacidade técnico-operacional da empresa licitante, limitado a 2 (dois) atestados por Grupo do objeto;

3.3.10.3. A apresentação de atestado(s) de capacidade técnica será obrigatória para as licitantes dos Grupos 1 e 2 do presente certame;

3.3.10.4. A exigência de atestado de capacidade técnica tem o objetivo de comprovar a aptidão das empresas no desempenho de atividade nos termos do objeto da presente licitação;

3.3.10.5. Deverão constar do(s) atestado(s) de capacidade técnica, apresentados pelas licitantes, os seguintes dados: identificação do emitente, especificação completa do fornecimento e/ou serviço executado, local e data de expedição, data de início e término do contrato. Além disso, também deverá constar no(s) documento(s) o endereço e telefone dos atestadores, ou qualquer outra forma com a qual o CONTRATANTE possa valer-se para realizar eventuais diligências;

3.3.10.6. Caso entenda necessário, o pregoeiro, por meio de diligência, poderá solicitar ao LICITANTE a comprovação da legitimidade dos atestados apresentados, devendo o licitante disponibilizar todas as informações pertinentes, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual do contratante e local em que foram prestados os serviços.

3.4. Margem de preferência

3.4.1. Lei 8.248/1991: Apesar do enquadramento do objeto no previsto no inciso II do art. 16-A, que possibilita a aplicação de margens de preferência para produtos de tecnologia da informação, a presente licitação adotará a margem de preferência zero. Esta decisão é justificada uma vez que os *appliances* F5 BIG-IP, tanto físicos quanto virtuais, possuem fabricação em território estrangeiro – especificamente no México para o hardware – e o desenvolvimento de seu software ocorre majoritariamente nos Estados Unidos e em outras localidades globais, conforme é possível verificar nos

documentos (Anexo Certificados Margem de Preferência id. 0742220) BIG-IP rSeries Certificate of Origin ([Certificate of Origin - BIG-IP rSeries.pdf](#)) e BIG-IP VE COO Statement ([BIG-IP VE COO Statement.pdf](#)), publicados no endereço eletrônico do fabricante: [F5 manufacturing compliance and certifications](#). Desta forma, a aplicação de qualquer percentual de margem de preferência não se alinha ao objetivo de fomento à indústria nacional, dado o caráter estrangeiro do bem e de seu desenvolvimento, e desvirtuaria a competitividade do certame.

3.4.2. Decreto 8.538/2015:

3.4.2.1. Não se aplicam as disposições do decreto, pois segundo o previsto no inciso I, do § 1º, do art. 4º, da Lei 14.133/2021, as disposições do decreto não são aplicadas "no caso de licitação para aquisição de bens ou contratação de serviços em geral, ao item cujo valor estimado for superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte". Desta forma como o custo dos grupos objeto deste TR ultrapassam o valor de R\$ 4.800.000,00 (quatro milhões oitocentos mil reais), disposto no inciso II, do art. 3º, da Lei Complementar 123/2006, afasta-se a aplicação do decreto.

3.5. Vistoria

3.5.1. A licitante poderá vistoriar o local onde serão executados os serviços até o último dia útil anterior à data fixada para a abertura da sessão pública, com o objetivo de inteirar-se das condições e grau de dificuldade existentes, mediante prévio agendamento de horário, com antecedência mínima de 48 (quarenta e oito) horas, junto ao departamento de Tecnologia da Informação dos órgãos partícipes, de 14 às 18 horas, limitada a realização da vistoria a um interessado por vez. O agendamento deverá ser realizado por meio dos seguintes contatos:

3.5.1.1. CJF: *e-mail* sutec@cjf.jus.br ; ou telefone (61) 3022-7400;

3.5.1.2. TRF3: *e-mails* ranu@trf3.jus.br e dinc@trf3.jus.br; ou telefones (11) 3012-1954 e (11) 3012-2280;

3.5.1.3. TRF5: *e-mail* seginfo@trf5.jus.br; ou telefone (81) 3425.9443;

3.5.1.3 JFAL: nti@jfal.jus.br; ou telefone (82) 2122-4233;

3.5.1.3 JFCE: nti@jfce.jus.br; (88) 3571-1385;

3.5.1.3 JFPB: atendimentonti@jfpb.jus.br; (83) 3690-1000;

3.5.1.3 JFPE: nti@jfpe.jus.br; (81) 3213-6292;

3.5.1.3 JFRN: nti@jfrn.jus.br; (84) 4005-7654

3.5.1.3 JFSE: ntic.atendimento@jfse.jus.br; (79) 3216-2200

3.5.1.4. TRF6: *e-mail* arianne.carmo@trf6.jus.br; ou telefone (31) 3501-1201.

3.5.2. A vistoria poderá ser substituída por uma declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação. Não serão admitidas, em hipótese alguma, alegações posteriores de desconhecimento da complexidade dos serviços e de dificuldades técnicas não previstas:

3.5.3. Caso a licitante deseje realizar o procedimento de vistoria, deverá fazê-lo na sede dos órgãos partícipes ou nas seções judiciárias, conforme detalhado no item 4.13 (Local da execução contratual).

3.5.3.1. No caso do GRUPO 2 (TRF5), especificamente, por se tratar de solução virtualizada, a vistoria poderá ser realizada de maneira remota;

4. Modelo de execução e de gestão do contrato (Art. 6º, XXIII, "f", Lei n. 14.133/2021)

4.1. Vigência (Art. 105, Lei n. 14.133/2021)

4.1.1. Ata de Registro de Preços: 01 (um) ano, contado do primeiro dia útil subsequente à data de divulgação no PNCP, e poderá ser prorrogado por igual período, desde que comprovado que o preço é vantajoso, mediante pesquisa de preços, nos termos do art. 84 da Lei n. 14.133, de abril de 2021 e do art. 22 do Decreto n. 11.462, de março de 2023.

4.1.1.1 Os quantitativos devem ser renovados quando da prorrogação da ata.

4.1.2. A vigência do contrato firmado com a empresa vencedora do certame será de:

a) De até 03 (três) meses, contados da assinatura do contrato, para a execução, mediante a emissão da Ordem de Serviço e Fornecimento de Bens, dos serviços de fornecimento/entrega, instalação e configuração da solução ADC, bem como o Recebimento Definitivo por parte do CONTRATANTE, para o GRUPO 1 e para o GRUPO 2;

b) 60 (sessenta) meses, para os demais serviços relativos ao GRUPO 1 do objeto, contados da data de emissão do Termo de Recebimento Definitivo - TRD, referente à prestação dos serviços de garantia e suporte técnico mensal, transferência de conhecimento, bem como dos serviços técnicos especializados de customização da solução, podendo ser prorrogado

nos limites da lei;

c) 12 (doze) meses, para os demais serviços relativos ao GRUPO 2 do objeto, contados da data de emissão do Termo de Recebimento Definitivo - TRD, referente à prestação dos serviços de suporte técnico mensal, transferência de conhecimento, bem como dos serviços técnicos especializados de customização da solução, podendo ser prorrogado nos limites da lei.

4.1.2.1 Justificativa: No caso do GRUPO 1, relativo à solução ADC composta por *appliances* físicos, o período de vigência de 60 (sessenta) meses contínuos para execução dos serviços se dá, sobretudo, para que a contratação seja atrativa para o mercado, favorecendo a Administração em termos de economicidade e ampliação da competitividade. Deve-se considerar ainda que os serviços contínuos são imprescindíveis ao bom funcionamento da solução ADC, e se paralisados, podem pôr em risco a continuidade das atividades do CJF. Portanto, um período maior de vigência minimiza o risco para o CONTRATANTE. Ainda, considerando que a vida útil desses equipamentos é em média de 5 anos, foi sugerida a garantia e suporte técnico de 60 (sessenta) meses para o item 1.1 do objeto. Quanto à duração da garantia, é fortemente recomendável que os ativos de TI estejam cobertos por garantia técnica durante toda sua vida útil, de modo a garantir o máximo aproveitamento do investimento e manter sua disponibilidade tecnicamente assegurada.

4.1.3 Impende, ainda, assinalar que os ativos que integram a solução de backup são comumente contratados no setor privado com cobertura de serviços em caráter plurianual, considerando o tempo de vida útil da tecnologia empregada. Em âmbito governamental, esta prática é igualmente adotada, conforme se verifica nos excertos das Boas Práticas, Orientações e Vedações para Contratação de Ativos de TIC – Versão 4 do Ministério do Planejamento, Desenvolvimento e Gestão, abaixo correlacionadas:

1.ORIENTAÇÕES ESPECÍFICAS

1.1. ESCOLHA DO POSICIONAMENTO ADEQUADO DA TECNOLOGIA

1.1.1. Para se garantir economicidade nas aquisições de ativos de TI, deve-se buscar definir as especificações técnicas de modo a posicionar a aquisição adequadamente dentro do ciclo de vida do bem.

[...]

1.4. ORIENTAÇÕES ESPECÍFICAS SOBRE CICLO DE VIDA

[...]

1.4.5. SERVIDORES DE REDE, APLICAÇÃO, EQUIPAMENTOS DE BACKUP, ARMAZENAMENTO, SEGURANÇA, ENTRE OUTROS

1.4.5.1. Para aquisição de servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros, deve-se considerar o tempo de vida útil mínimo de 5 (cinco) anos para fins de posicionamento da tecnologia e de garantia de funcionamento.

4.1.4 Ademais, cumpre mencionar que o ADC se traduz em uma solução de missão crítica, a qual possui uma alta complexidade de instalação, sendo que sua eventual paralisação pode pôr em risco a continuidade dos serviços informatizados e das atividades da Justiça Federal como um todo, o que reforça a característica plurianual de sua contratação, de modo que sua futura substituição, ao término de seu ciclo de vida útil, seja adequadamente planejada e operacionalizada pela Secretaria de Tecnologia da Informação deste CJF.

4.1.5 Por fim, cabe destacar que a celebração ora proposta de 5 anos para a avença encontra-se aderente ao disposto no inciso I do art. 40 da Lei n. 14.133/2021, o qual estabelece que o planejamento de compras deverá observar as condições de aquisição e pagamentos semelhante às do setor privado.

4.2. Reajuste (Art. 6º, LIX, Lei n. 14.133/2021)

4.2.1. Após o interregno de um ano, contado da data do valor estimado, os preços iniciais poderão ser reajustados, mediante negociação entre as partes, tendo como referência o limite máximo a variação acumulada do Índice de Custo da Tecnologia da Informação (ICTI), calculado e divulgado pelo IPEA;

4.2.2. No primeiro reajuste, as partes observarão para que o percentual a ser aplicado não seja superior à variação acumulada, no período compreendido entre o mês do orçamento estimado e aquela em que se verificar o mês anterior ao aniversário deste orçamento;

4.2.3. Os reajustes seguintes serão calculados considerando-se a variação acumulada dos 12 (doze) últimos meses anteriores ao aniversário do orçamento;

4.2.4. Caso o índice estabelecido para delimitar o reajustamento dos preços seja extinto ou, de qualquer forma, não possa mais ser utilizado para esse fim, as partes desde já concordam que em substituição seja adotado o que vier a ser determinado pela legislação então em vigor;

4.2.5. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice para delimitar o

reajustamento dos preços;

4.2.6. Incumbe à CONTRATADA a apresentação do pedido de reajuste acompanhado da respectiva memória de cálculo, a qual, após análise e aprovação pelo CONTRATANTE, redundará na emissão do instrumento pertinente ao reajuste contratual.

4.3. Obrigações contratuais da do Contratante e da Contratada

4.3.1. Deveres e responsabilidades do Contratante

4.3.1.1. Acompanhar e fiscalizar a execução do objeto contratual;

4.3.1.2. Determinar responsável para o acompanhamento e fiscalização da execução do objeto contratual;

4.3.1.3. Informar à CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados;

4.3.1.4. Comunicar oficialmente à CONTRATADA sobre quaisquer falhas e/ou anormalidades verificadas no cumprimento das obrigações contratuais;

4.3.1.5. Avaliar todos os serviços prestados pela CONTRATADA;

4.3.1.6. Responsabilizar-se pelos pagamentos dos serviços prestados pela CONTRATADA mediante a apresentação de Nota Fiscal;

4.3.1.7. Indicar os seus representantes para fins de contato e demais providências inerentes à execução do contrato;

4.3.1.8. Para os serviços inclusos no período de garantia do objeto e para a realização de suporte técnico, o CONTRATANTE permitirá o acesso dos técnicos habilitados e identificados da CONTRATADA às instalações onde se encontrarem os equipamentos. Esses técnicos ficarão sujeitos a todas as normas internas de segurança do CONTRATANTE, inclusive àqueles referentes à identificação, trânsito e permanência em suas dependências.

4.3.1.9 Deverá ser apresentada, concomitante à nota fiscal, a seguinte documentação:

- a) Certificado de Regularidade do FGTS - CRF, comprovando regularidade com o FGTS;
- b) Certidão Conjunta Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, expedida pela Secretaria da Receita Federal;
- c) Certidão Negativa de Débitos Trabalhistas - CNDT, expedida pela Justiça do Trabalho;
- d) Prova de regularidade com as Fazendas Estadual e Municipal do domicílio ou sede da CONTRATADA.

4.3.2. Deveres e responsabilidades da Contratada

4.3.2.1. Fornecer os *softwares* e equipamentos da solução com todos os itens acessórios necessários à sua perfeita instalação, acomodação, funcionamento e integração ao ambiente computacional do CONTRATANTE, incluindo, mas não limitando-se a cabos, adaptadores, conectores, transceivers, prateleiras, bandejas, trilhos, PDU e respectivas licenças de utilização em equipamentos de rede, interfaces, suportes, drivers de controle e programas de configuração.

4.3.2.2. Acatar as normas e diretrizes estabelecidas pelo CONTRATANTE para o fornecimento dos produtos e execução dos serviços objeto deste Termo de Referência.

4.3.2.3. Submeter à prévia aprovação do CONTRATANTE toda e qualquer alteração pretendida na prestação dos serviços.

4.3.2.4. Manter, durante a execução do contrato a ser firmado, as condições de habilitação e qualificação exigidas na licitação.

4.3.2.5. Sujeitar-se à fiscalização do CONTRATANTE, no tocante ao fornecimento e a prestação dos serviços, prestando todos os esclarecimentos solicitados e atendendo de imediato às reclamações fundamentadas, caso venham a ocorrer.

4.3.2.6. Prestar as atividades objeto da licitação, por meio de mão de obra especializada e devidamente certificada pelos fabricantes dos softwares e equipamentos da solução.

4.3.2.7. Indicar profissional que atuará, desde o início da execução do contrato até a conclusão da implantação, como Gerente de Projeto.

4.3.2.8. Propor os ajustes necessários à adequação, segurança e racionalização dos serviços prestados, respeitando o objeto deste Termo de Referência.

4.3.2.9. Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Termo de Referência, inclusive salários de pessoal, alimentação, diárias, hospedagem, transporte e seguros, bem como tudo que as leis trabalhistas e previdenciárias preveem e demais exigências legais para o exercício da atividade objeto deste Termo de Referência.

4.3.2.10. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e

produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação das penalidades previstas, caso os prazos e condições não sejam cumpridos.

4.3.2.11. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento para cobrança de pagamentos adicionais ao CONTRATANTE ou a não prestação satisfatória dos serviços.

4.3.2.12. Guardar inteiro sigilo dos dados que tiver acesso, reconhecendo serem estes de propriedade exclusiva do CONTRATANTE.

4.3.2.13. Substituir imediatamente, a critério do CONTRATANTE, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional do seu corpo técnico cuja presença seja considerada indesejável ou inconveniente, em virtude de comportamento inadequado devidamente justificado.

4.3.2.14. A CONTRATADA será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato.

4.3.2.15. Sujeitar-se a mais ampla e irrestrita fiscalização, por parte da Equipe de Fiscalização e/ou Recebimento indicada pelo CONTRATANTE para acompanhamento da execução do contrato, prestando todos os esclarecimentos que lhes forem solicitados e atendendo às reclamações formuladas.

4.3.2.16. Comunicar a Equipe de Fiscalização e/ou Recebimento, por escrito, qualquer anormalidade que ponha em risco o fornecimento ou a execução dos serviços.

4.3.2.17. Corrigir as falhas detectadas pela Equipe de Fiscalização e/ou Recebimento indicada pelo CONTRATANTE.

4.3.2.18. Executar as atividades previstas no contrato em estrito cumprimento aos prazos previstos no ANEXO IV – CRONOGRAMA DE IMPLANTAÇÃO, após a emissão de Ordem de Serviço e Fornecimento de Bens (OSFB) pelo CONTRATANTE.

4.3.2.19. Cumprir as exigências de reserva de cargos previstas em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz.

4.4. Papéis a serem desempenhados durante a execução contratual

4.4.1. Pelo CONTRATANTE

4.4.1.1. Equipe de Fiscalização do Contrato: os produtos e serviços objetos desta contratação serão fiscalizados por servidor ou comissão de servidores do CONTRATANTE, doravante denominados Equipe de Fiscalização, que terá autoridade para exercer toda e qualquer ação de orientação geral, controle e fiscalização da execução contratual;

4.4.1.1.1. Compete, à Equipe de Fiscalização, dentre outras atribuições:

a) Solicitar à Contratada e seus prepostos, ou obter da Administração, tempestivamente, todas as providências necessárias ao bom andamento do contrato e anexar aos autos do processo correspondente cópia dos documentos escritos que comprovem essas solicitações de providências;

b) Manter organizado e atualizado um sistema de controle em que se registrem as ocorrências ou os serviços descritos de forma analítica;

c) Acompanhar e atestar a prestação dos serviços contratados e indicar a ocorrência de inconformidade desses serviços ou não cumprimento do contrato;

d) Encaminhar à Secretaria de Administração os documentos para exame e deliberação sobre a possível aplicação de sanções administrativas.

4.4.1.1.2. A ação da Equipe de Fiscalização não exonera a CONTRATADA de suas responsabilidades contratuais.

4.4.2. Pela CONTRATADA

4.4.2.1. Representante legal: pessoa formalmente designada e devidamente autorizada a firmar contrato em nome da CONTRATADA.

4.4.2.2. Preposto: nomeado pelo representante legal no início da execução contratual, nos termos do art. 118 da Lei nº 14.133/21, que atuará como representante da CONTRATADA durante a execução contratual. Deverá ser apresentado, por ocasião da Reunião Inicial de Planejamento, conforme cronograma constante do ANEXO IV.

4.4.2.3. Gerente de Projetos: líder e responsável pela entrega dos serviços de planejamento e implantação da solução, de modo a garantir a qualidade dos resultados e o atendimento aos requisitos e prazos estipulados no Edital. Deverá ser apresentado, por ocasião da Reunião Inicial de Planejamento, conforme cronograma constante do ANEXO IV.

4.4.2.4. Responsável Técnico: funcionário da empresa responsável pela prospecção, elaboração e implantação da solução além de responder por questões técnicas atinentes à solução durante a execução contratual. Deverá ser apresentado, por

ocasião da Reunião Inicial de Planejamento, conforme cronograma constante do ANEXO IV.

4.5. Qualificação técnica dos profissionais da contratada

4.5.1. O Gerente de Projetos deve atender no mínimo aos seguintes requisitos abaixo arrolados e apresentado no prazo estabelecido em cronograma (ANEXO IV):

- a) Deve possuir escolaridade de nível superior completo;
- b) Deve possuir certificação PMP – Project Management Professional – do PMI – Project Management Institute – ou possuir MBA – Master of Business Administration – em Gerência de Projetos.

4.6. Dinâmica de execução contratual

4.6.1. Execução contratual

4.6.1.1. A CONTRATADA deverá iniciar a execução das atividades de entrega, instalação e configuração dos equipamentos e *softwares* da solução a partir da emissão da Ordem de Serviço e Fornecimento de Bens (OSFB) pelo CONTRATANTE, conforme cronograma constante do ANEXO IV - CRONOGRAMA DE IMPLANTAÇÃO;

4.6.1.2. A CONTRATADA deverá entregar todos os equipamentos, *softwares* embarcados, licenças de uso e quaisquer outros acessórios da solução no prazo máximo de até 45 (quarenta e cinco) dias corridos, a contar da data de emissão da Ordem de Serviço e Fornecimento de Bens (OSFB), conforme cronograma constante do ANEXO IV;

4.6.1.2.1 Não será permitida a entrega parcial dos equipamentos e demais elementos que compõem a solução, devendo a CONTRATADA entregar em sua totalidade o quantitativo solicitado na Ordem de Serviço e Fornecimento de Bens (OSFB) emitida pelo CONTRATANTE, podendo a CONTRATADA incorrer em sanção contratual;

4.6.1.3. A CONTRATADA e o CONTRATANTE deverão realizar, em até 5 (cinco) dias corridos após a emissão da Ordem de Serviço e Fornecimento de Bens (OSFB), a Reunião Inicial de Planejamento, a ser realizada, preferencialmente, no formato presencial, na sede do CONTRATANTE, ou remotamente, por meio de videoconferência, conforme cronograma do ANEXO IV.

4.6.1.3.1. A reunião terá como objetivo apresentar a metodologia de trabalho, planejamento e coordenação das atividades de entrega da solução contratada;

4.6.1.3.2. Os detalhes quanto ao formato, data e horário da reunião deverão ser acordados com o CONTRATANTE por meio dos contatos constantes da Ordem de Serviço e Fornecimento de Bens (OSFB).

4.6.1.4. A CONTRATADA deverá apresentar o Plano de Implantação, em até 10 (dez) dias corridos contados da realização da Reunião Inicial de Planejamento, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos *softwares* e equipamentos da solução, conforme cronograma constante do ANEXO IV;

4.6.1.5. A CONTRATADA deverá realizar a instalação e configuração dos equipamentos e *softwares* embarcados da solução, incluindo suas licenças de uso, no prazo máximo de 20 (vinte) dias corridos, contados a partir da data de emissão do primeiro Termo de Recebimento Provisório (TRP1), em conformidade com o cronograma apresentado no ANEXO IV;

4.6.1.5.1. A conclusão das etapas de instalação e configuração dos equipamentos e *softwares* embarcados da solução, bem como a entrega das licenças de uso, deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE;

4.6.1.6. Finalizada a etapa de instalação e configuração da solução, o que será formalizado por meio da emissão do Termo de Recebimento Definitivo (TRD) por parte do CONTRATANTE, começará a vigorar o prazo de vigência contratual, conforme disposto no item 4.1.2 deste Termo;

4.6.1.7. Na hipótese de ser verificada a inadequação do objeto com relação aos requisitos e descrição detalhados neste Termo de Referência, nas etapas de entrega ou de implantação e configuração da solução, a Equipe de Fiscalização Técnica ou o Gestor o rejeitará imediatamente, no todo ou em parte, devendo a CONTRATADA proceder à regularização no prazo máximo de 15 (quinze) dias corridos contados da notificação pelo CONTRATANTE;

4.6.1.8. Após a emissão do Termo de Recebimento Definitivo (TRD) será dado início à prestação do serviço de suporte técnico, o qual será aferido mensalmente, e se estenderá por toda a vigência contratual. Assim, a data de emissão do TRD pelo CONTRATANTE será considerada como o marco inicial para a aferição do suporte técnico, o qual terá pagamentos mensais, segundo critérios estabelecidos no item 4.8 - Critérios de medição e pagamento deste Termo;

4.6.1.8.1. O dia do mês em que ocorrer a emissão do TRD será o marco inicial para a contagem dos períodos mensais relativos ao serviço de suporte técnico. Assim, cada período mensal se iniciará no dia indicado pela emissão TRD e se estenderá até o dia anterior do mês subsequente. Exemplo: se o TRD for emitido no dia 10 de um certo mês, então cada período mensal sempre se iniciará no dia 10 de cada mês e se estenderá até o dia 9 do mês subsequente.

4.6.1.9. Ao longo da vigência contratual, o CONTRATANTE emitirá Ordem(ns) de Serviço específica(s) para a ação de transferência de conhecimento, conforme descrito no item 4.6.6;

4.6.1.10. Ao longo da vigência contratual, o CONTRATANTE poderá emitir Ordem(ns) de Serviço específica(s) para os serviços técnicos especializados para implementação e customização da solução, sob demanda e sem garantia de utilização mínima de utilização dos serviços, conforme descrito no item 4.6.7 deste Termo.

4.6.2. Plano de Implantação

4.6.2.1. A CONTRATADA deverá elaborar Plano de Implantação da solução contendo cronograma de execução das atividades, previsão de recursos, pessoas envolvidas e atividades a serem desenvolvidas pela CONTRATADA, além de indicar os principais riscos e suas respectivas formas de mitigação, contendo também os seguintes itens:

4.6.2.1.1. Descrição e detalhamento dos procedimentos para entrega, retirada das embalagens e conferência dos equipamentos, *softwares* embarcados e acessórios entregues;

4.6.2.1.2. Descrição e detalhamento das informações sobre as etapas de instalação física dos equipamentos incluindo distribuição dos equipamentos pelos racks, movimentação de equipamentos existentes, conexões elétricas e lógicas necessárias, definição de nomes dos equipamentos e de endereçamento de gerência IP;

4.6.2.1.3. Proposta de interconexão física e lógica dos componentes da solução aos ativos rede do CONTRATANTE, observando as melhores práticas de segurança e considerando os recursos disponíveis nos elementos da solução;

4.6.2.1.4. Planejamento da engenharia de tráfego da solução com base nas melhores práticas de segurança e considerando os recursos disponíveis nos elementos da solução;

4.6.2.1.5. Descrição e detalhamento das condições de *rollback* de cada mudança no ambiente do CONTRATANTE para a instalação da solução;

4.6.2.1.6. Descrição e detalhamento das atividades de teste de operação da solução e planos de testes para os diversos componentes da solução que comprovem o funcionamento das regras e configurações aplicadas, bem como dos recursos de tolerância a falhas dos *softwares* e equipamentos da solução;

4.6.2.1.7. Descrição e detalhamento da ação de Transferência de Conhecimento, nos termos do item 4.6.6 deste documento.

4.6.3. Serviço de instalação e configuração da solução ADC

4.6.3.1. As atividades de entrega, instalação e configuração dos equipamentos e/ou *softwares* da solução deverão ocorrer na sede do CONTRATANTE (ou nas unidades da federação, quando se aplicar), conforme item 4.13 (Local da execução contratual), e os serviços de implantação ou quaisquer outros que possam causar instabilidade no ambiente de produção devem ser realizados em horários fora do expediente do órgão e previamente agendados com a Equipe de Fiscalização do Contrato;

4.6.3.1.1. Ficará sob responsabilidade da CONTRATADA o remanejamento dos equipamentos entre os endereços descritos no item 4.13 (Local da execução contratual), a qualquer momento, durante toda a vigência contratual, nos casos em que for necessária a movimentação dos *appliances* físicos para atender às necessidades do CONTRATANTE.

4.6.3.2. O CONTRATANTE poderá autorizar a realização de atividades durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento dos serviços e aplicações em ambiente de produção;

4.6.3.3. O processo de entrega, instalação e configuração dos componentes da solução deverá ser acompanhado e supervisionado pela equipe técnica indicada pelo CONTRATANTE;

4.6.3.4. A CONTRATADA deverá entregar os equipamentos novos de 1º uso juntamente com todos os itens acessórios de *hardware* e de *software* necessários à perfeita instalação e funcionamento, incluindo cabos, conectores, interface, suportes, drivers de controle, programas de configuração, conforme especificações constantes no ANEXO I - DETALHAMENTO DOS REQUISITOS TÉCNICOS DO OBJETO PARA O GRUPO 1 - deste Termo de Referência;

4.6.3.4.1. Para a solução de ADC virtual, relativa ao do Grupo 2 do objeto desta contratação, a CONTRATADA deverá entregar todos os *softwares* e seus respectivos licenciamentos/subscrições conforme especificações constantes do ANEXO II - DETALHAMENTO DOS REQUISITOS TÉCNICOS DO OBJETO PARA O GRUPO 2 deste Termo de Referência.

4.6.3.5. Entregar os equipamentos devidamente protegidos e embalados, originais lacrados, sem danos de transporte e manuseio;

4.6.3.6. Entregar os equipamentos e/ou *softwares*, às suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos fornecidos;

4.6.3.7. Entregar toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização, na data de início da prestação dos serviços previstos na Ordem de Serviço inicial;

4.6.3.8. Caso a implantação de qualquer elemento da solução cause interferência na correta operação da rede de dados do CONTRATANTE, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou

retornar ao ambiente à condição anterior à implantação, em até 12 (doze) horas;

4.6.3.9. A execução dos serviços de entrega, instalação e configuração dos equipamentos e/ou *softwares* da solução deverá contemplar, no mínimo, os seguintes itens:

4.6.3.9.1. Instalação física e ativação dos componentes da solução, quando se tratar de solução ADC física, ou instalação em servidores virtuais, quando se tratar de solução ADC virtual, nos *data centers* do CONTRATANTE;

4.6.3.9.2. Integração à rede do CONTRATANTE, sem interrupção no funcionamento normal dos serviços de TI. Caso exista a necessidade de interrupção de qualquer equipamento ou serviço em produção para a integração da solução, o prazo para realização e a duração da janela de manutenção deverão ser acordados com o CONTRATANTE;

4.6.3.9.3. Instalação e configuração dos *softwares* e funcionalidades exigidas na especificação técnica dos elementos que compõem a solução fornecida, bem como quaisquer outras disponíveis adicionalmente nos diversos componentes da solução mediante solicitação da equipe do CONTRATANTE;

4.6.3.9.4. Realização de testes de operação da solução que comprovem o funcionamento dos recursos de tolerância a falhas dos diversos componentes da solução, quando aplicável;

4.6.3.9.5. Atualização do Plano de Implantação com todas as informações que representem a topologia física e lógica e a configuração final aplicadas.

4.6.4. Serviço de suporte técnico

4.6.4.1. O serviço de suporte técnico para os *appliances* físicos e *softwares* que compõem a solução do GRUPO 1 do objeto deverá ser executado pela CONTRATADA, durante o prazo de 60 (sessenta) meses da vigência contratual, de maneira presencial, contados a partir da data de emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos equipamentos e *softwares* embarcados da solução;

4.6.4.1.1. O serviço de suporte técnico referente ao GRUPO 1 desta contratação poderá ser prestado de maneira remota, excepcionalmente, a critério do CONTRATANTE;

4.6.4.2. O serviço de suporte técnico para os *appliances* virtuais que compõem a solução do GRUPO 2 do objeto deverá ser executado pela CONTRATADA, durante o prazo de 60 (sessenta) meses da vigência contratual, de maneira remota, contados a partir da data de emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos equipamentos e *softwares* embarcados da solução;

4.6.4.3. O serviço de suporte técnico para os GRUPOS 1 e 2 desta contratação serão iniciados imediatamente após a emissão do Termo de Recebimento Definitivo (TRD), conforme cronograma do ANEXO IV, e se encerrarão juntamente com o término da vigência contratual.

4.6.4.4. O serviço de suporte técnico da solução consiste em:

4.6.4.4.1. Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, no local de instalação da solução, visando a solução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução, permitindo o retorno à condição normal de operação.

4.6.4.4.2. Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, por meio de contato telefônico ou outro recurso de comunicação, visando o esclarecimento de dúvidas em relação a qualquer elemento da solução.

4.6.4.4.3. No caso de solução composta por *appliances* físicos (GRUPO 1), realizar visitas técnicas preventivas no local de instalação da solução (*on-site*), com frequência mensal, e com duração de pelo menos 1 (uma) hora de duração por visita, visando assegurar o melhor desempenho da solução.

4.6.4.4.4. No caso de solução composta por *appliances* virtuais (GRUPO 2), realizar inspeções técnicas preventivas de maneira remota, com frequência mensal, e com duração de pelo menos 1 (uma) hora por inspeção, visando assegurar o melhor desempenho da solução.

4.6.4.4.5. Substituir peças e componentes, cujos problemas sejam decorrentes do desgaste pelo uso normal dos equipamentos, por outras de configuração idêntica ou superior, originais e novas, conforme previsto na garantia da solução, no prazo estabelecido no item 4.12.8.2.

4.6.4.4.6. Atualizar a solução, sempre que solicitado pela CONTRATANTE, quando do lançamento de novas versões ou de firmwares que corrijam vulnerabilidades conhecidas ou defeitos do software ou hardware.

4.6.4.5. O CONTRATANTE realizará a abertura de chamados técnicos de suporte por ligação telefônica, por *e-mail* ou via Internet, em período integral, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

4.6.4.6. A CONTRATADA deverá informar o procedimento para abertura de chamado técnico de suporte no documento Plano de Implantação.

4.6.4.7. Se a Central de Suporte estiver localizada fora de Brasília, a CONTRATADA deverá informar o DDG (discagem direta gratuita 0800). O acesso à área restrita de suporte em sítio eletrônico da Internet deverá estar disponível, também,

24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

4.6.4.8. Quando da abertura de chamado técnico de suporte pelo CONTRATANTE, a CONTRATADA deverá informar, para fins de controle, o número do chamado.

4.6.4.9. A CONTRATADA deverá enviar mensalmente, conforme estabelecido no item 4.7.1.15.1, ou disponibilizar acesso por meio do Portal da Internet, a relação consolidada dos chamados abertos no período mensal, mencionando minimamente o seguinte: número do chamado técnico, data e hora de abertura do chamado, problemas verificados pelo técnico da CONTRATADA durante a resolução do chamado, medidas adotadas para a resolução dos problemas, eventuais pendências a serem solucionadas pelo CJF e nome do técnico responsável pelo atendimento;

4.6.4.10. A CONTRATADA deverá disponibilizar acesso a base de conhecimento do fabricante dos componentes da solução, na data de início da prestação dos serviços previstos na Ordem de Serviço inicial, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, com pesquisa efetuada através de ferramentas de busca) e atualizações;

4.6.4.11. A CONTRATADA deverá realizar a cada ocorrência, como escopo das atividades de visitas/inspeções técnicas preventivas, as tarefas de coleta e análise de logs dos produtos, realizar o levantamento de configurações aplicadas nos equipamentos e *softwares* embarcados da solução, buscando compará-las às melhores práticas e recomendações dos fabricantes, avaliar aspectos de segurança e desempenho da solução, finalizando com a elaboração de relatório técnico com as informações coletadas e as recomendações a serem aplicadas à solução;

4.6.4.12. Para o disposto no item anterior, o técnico da CONTRATADA deverá levar em consideração a realidade do ambiente de servidores e aplicações do CJF (*as-is*), visando otimizar o funcionamento da solução por meio de ações que atendam às necessidades e aos objetivos do CONTRATANTE (*to-be*);

4.6.4.13. As visitas/inspeções técnicas preventivas deverão ser realizadas, mensalmente, por técnico(s) plenamente qualificado(s), com declaração emitida pelos fabricantes dos equipamentos e/ou *softwares* da solução ofertada ou ter registro no site do fabricante, e deverão ser prestadas com acompanhamento da equipe técnica do CONTRATANTE;

4.6.4.14. A contagem de prazo para a realização das visitas/inspeções técnicas preventivas será iniciada após emissão do Termo de Recebimento Definitivo, devendo ocorrer automaticamente em dia e hora previamente agendada com o CONTRATANTE e serão consideradas concluídas após o entrega do relatório técnico de atendimento e aceite pelo CONTRATANTE. A cada visita/inspeção deverá ser gerado relatório técnico com sugestões e ajustes para a melhoria de desempenho, funcionalidade e segurança;

4.6.4.15. A CONTRATADA deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CONTRATANTE, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações.

4.6.4.16. O serviço de suporte técnico especializado, deverá ser prestado por localidade segundo endereços definidos no item 4.13 - Local da execução contratual, independente do quantitativo de equipamentos e/ou *softwares* a serem fornecidos/implantados no site. Dessa forma, tal serviço não deverá ser majorado ou ajustado em casos de aquisições "tardias ou pontuais".

4.6.5. Níveis mínimos de serviço

4.6.5.1. Quando da abertura de chamados de suporte técnico pelo CONTRATANTE, cada chamado deverá ser categorizado em 3 (três) níveis, conforme mostrado na tabela a seguir, e deverá ser tratado conforme os prazos de início do atendimento e resolução do problema:

Criticidade	Descrição	Prazo máximo para início de atendimento (contados a partir da abertura do chamado)	Prazo máximo para restauração do serviço (contados a partir da abertura do chamado)
Severidade 1 (Alta)	Atuação ON-SITE em ocorrências que causem indisponibilidade ou restrição de funcionalidade da solução prejudicando a operação normal e que gerem impacto ao negócio.	Em até 2 (duas) horas deve ter um técnico da CONTRATADA ON-SITE.	Em até 4 (quatro) horas

Severidade 2 (Média)	Atuação REMOTA visando sanar problemas que criem restrições a operação normal da solução não gerando impacto ao negócio.	Em até 6 (seis) horas um técnico da CONTRATADA entra em contato.	Em até 12 (doze) horas
Severidade 3 (Baixa)	Atuação REMOTA visando sanar problemas que não afetem a operação normal da solução ou dúvidas de operação e configuração.	Em até 12 (doze) horas um técnico da CONTRATADA entra em contato.	Em até 36 (trinta e seis) horas

4.6.5.2. O não atendimento aos Níveis Mínimos de Serviço estabelecidos anteriormente acarretará aplicação de glosa sobre o custo mensal do serviço de suporte técnico, conforme item 4.10 (Glosas) deste Termo de Referência.

4.6.6. Transferência de conhecimento

4.6.6.1. A CONTRATADA deverá realizar a transferência de conhecimento, preferencialmente de forma remota, para o quantitativo de pessoas estabelecido por cada órgão partícipe do presente Sistema de Registro de Preços - SRP, conforme tabela do item 1, por meio de treinamento nas tecnologias da solução com carga horária mínima de, no mínimo, 40 (quarenta) horas;

4.6.6.1.1. Havendo o interesse, um ou mais órgãos partícipes poderão combinar de realizar a ação de Transferência de Conhecimento de forma conjunta e integrada, desde que respeitados os prazos estabelecidos no Termo de Referência, cabendo à CONTRATADA a organização das turmas;

4.6.6.1.2. O treinamento deverá ser realizado no formato *online*, em plataforma a ser definida e disponibilizada pela CONTRATADA;

4.6.6.1.3 O treinamento deverá ser realizado sempre em um único turno, preferencialmente o vespertino, de cada dia agendado;

4.6.6.2. O serviço de transferência de conhecimento deverá ser prestado somente após a emissão do Termo de Recebimento Definitivo (TRD) relativo às etapas de fornecimento, instalação e configuração da solução e será solicitado sob demanda, mediante a emissão de Ordem de Serviço – OS específica para este serviço;

4.6.6.2.1 Cada órgão partícipe do presente SRP emitirá a sua Ordem de Serviço, de maneira individualizada, para dar início à ação de Transferência de Conhecimento;

4.6.6.3. O CONTRATANTE poderá iniciar a solicitação dos serviços de transferência de conhecimento após 20 (vinte) dias corridos contados da emissão do TRD;

4.6.6.4. A Ordem de Serviço específica para a ação de transferência de conhecimento poderá ser emitida de maneira individualizada ou para grupos de alunos, a critério do CONTRATANTE, ao longo da vigência contratual, devendo indicar expressamente o nome de quais servidores realizarão a capacitação, conforme o cronograma previamente acordado entre as partes quando da realização da Reunião Inicial de Planejamento;

4.6.6.4.1. O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE na ocasião da Reunião Inicial de Planejamento e integrará o teor do Plano de Implantação a ser entregue pela CONTRATADA;

4.6.6.5. A CONTRATADA deverá estar apta a iniciar a ação de transferência de conhecimento em até 7 (sete) dias corridos, contados da emissão da Ordem de Serviço específica para esse serviço;

4.6.6.5.1. O CONTRATANTE emitirá as Ordens de Serviço em consonância com o cronograma da ação de treinamento constante do Plano de Implantação. Qualquer necessidade de alteração do cronograma deverá ser formalizada antecipadamente junto à CONTRATADA para reagendamento;

4.6.6.5.2. Caso a CONTRATADA fique impossibilitada quanto à realização da transferência de conhecimento solicitada na Ordem de Serviço, ela deverá informar por escrito ao CONTRATANTE, justificadamente, e agendar nova data. Neste caso, após avaliação das justificativas apresentadas, poderá ficar caracterizado o atraso na prestação do serviço e estará a CONTRATADA sujeita às sanções administrativas previstas neste Termo;

4.6.6.5.3. Havendo uma segunda impossibilidade de realizar a transferência de conhecimento solicitada por meio de Ordem de Serviço, será aplicada a multa moratória correspondente;

4.6.6.6. A CONTRATADA deverá concluir a ação de transferência de conhecimento ou, minimamente, disponibilizar todo o material do programa de capacitação, em até 45 (quarenta e cinco) dias corridos contados da emissão de cada Ordem de Serviço;

4.6.6.7. A ação de transferência de conhecimento poderá ser paga individualmente, à medida em que os servidores designados nas Ordens de Serviço concluírem as capacitações e houver a emissão dos certificados de conclusão, cabendo à CONTRATADA encaminhar ao Gestor do Contrato os documentos necessários para ateste da despesa;

4.6.6.8. O programa para a transferência de conhecimento deverá abordar as principais funcionalidades de administração e operação da solução e ser previamente aprovado pelo CONTRATANTE, e eventuais mudanças de conteúdo solicitadas deverão constar no material didático, em especial:

4.6.8.1 Apresentação da arquitetura da solução e dos conceitos fundamentais;

4.6.8.2 Aspectos sobre instalação da solução;

4.6.8.3 Configuração e gerenciamento da solução;

4.6.8.4 Operação completa da solução;

4.6.8.5 Análise de logs e problemas;

4.6.8.6 Geração e customização de relatórios, caso aplicável;

4.6.8.7 Verificação de alertas e tomada de ações;

4.6.8.8 Deduplicação de dados;

4.6.8.9 Segurança da Informação e da solução;

4.6.8.10 Otimizações ou desempenho (performance);

4.6.8.11 Troubleshooting.

4.6.6.12. A CONTRATADA deverá realizar laboratórios práticos que permitam exercitar os conteúdos acima

4.6.6.13. A ação de Transferência de Conhecimento deverá abranger, minimamente, os seguintes conteúdos:

a) Apresentação da arquitetura da solução e dos conceitos fundamentais;

b) Instalação e Configuração da Solução;

c) Conceitos e configuração de alta disponibilidade;

d) Conceitos de Segurança para Aplicações Web;

e) Vulnerabilidades comuns para aplicações Web;

f) Configurações de Políticas de Segurança;

g) Monitoramento do Tráfego de dados / rede;

h) Monitoramento de sessões e usuários;

i) Detecção de anomalias;

j) Solução de problemas básicos;

4.6.6.14. O material didático da transferência de conhecimento deverá ser disponibilizado em formato eletrônico, para todos os participantes, sem custo adicional para o CONTRATANTE, devendo ainda estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), tendo em vista que é comum soluções de Tecnologia da Informação serem desenvolvidas por empresas estrangeiras e material bilíngue.

4.6.6.15. Caberá à CONTRATADA o controle de participação no treinamento pelos servidores indicados pelo CONTRATANTE e, ao final, deverá entregar ao gestor do contrato a lista de presença dos participantes indicados;

4.6.6.16. Ao final da ação de Transferência de Conhecimento, a CONTRATADA deverá emitir certificado de participação ao final do curso a cada participante, detalhando programa o seguinte:

a) Nome da instituição de ensino (caso aplique-se);

b) Nome do curso/capacitação (caso aplique-se);

c) Nome completo do aluno capacitado;

d) Data de início e término da capacitação;

e) Carga horária;

f) Conteúdo programático (Ementa).

4.6.6.17 O instrutor designado para a ação de treinamento deverá possuir certificação emitida pelo fabricante dos equipamentos ADC, ou, alternativamente, poderá ser um profissional que atuou na etapa de implementação e configuração da solução. Essa comprovação deverá ser apresentada até 3 (três) dias úteis antes do início da execução do serviço, segundo demandado por Ordem de Serviço.

4.6.6.18. Caso a transferência de conhecimento não seja satisfatória com relação à profundidade do conteúdo apresentado

ou domínio dos temas por parte do instrutor, a CONTRATADA deverá complementar, sem ônus adicional, o repasse dos pontos considerados pelo CONTRATANTE como insatisfatórios.

4.6.6.19. A transferência de conhecimento deverá ser realizada por instrutor, segundo as mesmas características do item 4.6.6.12.

4.6.7. Serviços técnicos especializados sob demanda

4.6.7.1. Os serviços técnicos especializados para implementação e customização da solução ADC deverão ser prestados pela CONTRATADA ao CONTRATANTE, sob demanda, durante a vigência contratual;

4.6.7.1.1. Os serviços serão demandados pelo CONTRATANTE, por meio de Ordens de Serviço – OS, contendo o quantitativo estimado de horas de trabalho, o período de execução e a descrição dos serviços a serem executados;

4.6.7.1.2. O pagamento deverá ser realizado de acordo com a quantidade de horas efetivamente consumidas constante da OS. Qualquer alteração na quantidade de horas deverá ser justificada e previamente aprovada pelo CONTRATANTE;

4.6.7.1.3. Cada OS deverá ser precedida dos seguintes documentos, entregues pela CONTRATADA, para embasamento da quantidade de horas, agendamento, alocação de recursos e outras providências do CONTRATANTE:

a) Cronograma de execução preliminar: detalhando etapas e atividades, desdobradas no quantitativo estimado de horas (ou fração de hora) de trabalho, associado a cada tarefa que será executada, de acordo com metodologias de projetos/processos, como PMBOK e RUP. As entregas (relatórios, documentação técnica etc.), pertinentes ao serviço, não devem onerar o quantitativo de horas estimado neste cronograma de execução;

b) Arquitetura da solução, quando aplicável, nos casos de implantação nova funcionalidade: contendo diagramas da solução, descrição de funcionamento, especificações técnicas, requisitos e configurações necessárias, sempre considerando o contexto, os cenários adotados e as especificidades do ambiente computacional do CONTRATANTE;

d) Lista de recursos necessários, quando aplicável: como contas de acesso, conexões VPN, ferramentas e informações técnicas, para a execução das atividades pela Contratada no ambiente do CONTRATANTE;

d) Análise de risco: contendo a identificação de ameaças, causas e efeitos, probabilidades e impactos, e possíveis ações e medidas de tratamento, incluindo situações que poderão vir a demandar outras atividades não inicialmente estimadas

4.6.7.1.4. Cada unidade demandada para este serviço deverá corresponder a 01 (uma) hora de trabalho de um profissional da Contratada, que executará suas atividades conforme as áreas de atividades indicadas a seguir:

a) Implementação: execução das implantações, adaptações código, criação de infraestrutura e atividades relacionadas. Inclui os seguintes Part Numbers: GPS-AC - Associate Consultant; GPS-C – Consultant; GPS-SC - Senior Consultant; e GPS-PRCON - Principal Consultant;

b) Arquitetura: definição da arquitetura lógica e física do projeto, garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais. Inclui os seguintes Part Numbers: GPS-A – Architect; GPS-SA - Senior Architect; e GPS-PA - Principal Architect;

c) Gerenciamento de Projetos: gerenciamento do projeto de acordo com as práticas preconizadas pelo Guia PMBOK (Project Management Body of Knowledge) do Project Management Institute - PMI, considerando controle de prazos, escopo, esforço, recursos, qualidade, comunicação e riscos, além da elaboração de relatórios de posicionamento executivo, com indicadores de status do projeto, de modo a garantir sua efetividade, em relação ao serviço demandado. Inclui os seguintes Part Numbers: GPS-PC - Project Coordinator; GPS-PJM - Project Manager; e GPS-PRM - Program Manager.

4.6.7.1.5. Os serviços poderão ser prestados na modalidade presencial ou à distância (remotamente), a critério do CONTRATANTE, sendo esta modalidade definida na Ordem de Serviço, para cada perfil profissional a ser alocado;

4.6.7.1.6. Todos os profissionais especialistas alocados nos projetos e atividades demandadas deverão dispor das seguintes habilidades comportamentais:

a) Proatividade;

b) Comprometimento com prazos e qualidade;

c) Comunicação e interação ativa com as equipes de TI do CONTRATANTE;

d) Administração de conflitos e gerenciamento de pessoas (habilidade requerida apenas para os profissionais especialistas com perfil de “Gerenciamento de Projetos”).

4.6.7.1.7. Além das habilidades comportamentais descritas acima, os profissionais especialistas com perfil de “Implementação” também deverão:

a) Responder questionamentos técnicos pertinentes ao serviço executado;

b) Informar e explicar quanto à necessidade de eventuais ajustes e demais situações não inicialmente previstas;

c) Na ocasião de atuação à distância (teletrabalho), permanecer em sala virtual com ao menos 01 (um) integrante da

equipe técnica de TI do CONTRATANTE, compartilhando a visualização da tela (área de trabalho) em que está executando as atividades, durante os horários acordados para a realização do serviço demandado.

4.6.7.1.8. Previamente ao início de cada ação demandada, a CONTRATADA deverá realizar uma reunião de alinhamento inicial com o CONTRATANTE, conduzida pelo profissional com perfil de “Gerenciamento de Projetos”, na qual este deverá:

- a) Realizar um *briefing* do projeto/serviço a ser executado, incluindo o escopo e as restrições;
- b) Validar os recursos entregues pelo CONTRATANTE (contas de acesso, conexões VPN, ferramentas, informações técnicas, etc), quando aplicáveis, para a execução das atividades pelos profissionais especialistas em seu ambiente, bem como validar o acesso, de todos os profissionais alocados, às ferramentas de comunicação e colaboração adotadas pelo CONTRATANTE;
- c) Combinar com o CONTRATANTE os horários de atuação dos profissionais especialistas alocados.

4.6.7.1.9. Durante a execução do serviço, os profissionais especialistas alocados deverão:

- a) Atuar continuamente e em regime de dedicação exclusiva nos horários previamente acordados para a execução das atividades, não sendo permitido o compartilhamento do tempo destes profissionais para atuação simultânea em projetos/atividades de terceiros;
- b) Utilizar exclusivamente as ferramentas de comunicação e colaboração adotadas pelo CONTRATANTE

4.6.7.1.10. Em cada projeto, a CONTRATADA deverá ainda realizar as seguintes entregas:

- a) Periodicamente, ao final de cada semana de trabalho, em projetos executados durante mais de uma semana:
 - a.1) Relatório gerencial: com informações sobre o progresso das atividades, atualização do cronograma e indicadores de status do projeto.
 - b) Em até 05 (cinco) dias úteis após a efetiva conclusão das atividades:
 - b.1) Relatório gerencial final: com informações sobre as atividades, atualização do cronograma e indicadores de status do projeto;
 - b.2) Relatório de horas trabalhadas (*timesheet*): detalhando a alocação dos profissionais envolvidos nas datas e atividades efetivamente executadas;
 - b.3) Documentação técnica: novo documento do tipo “*as-built*” ou atualização da documentação existente, conforme o caso, refletindo os procedimentos, comandos e configurações efetivamente executadas, bem como o estado atual do ambiente/solução alvo dos serviços.

4.6.7.1.11. Somente será autorizado o faturamento das horas efetivamente consumidas na execução das atividades, de acordo com a validação realizada pelo CONTRATANTE, com base no acompanhamento diário das atividades e na análise dos entregáveis listados nos itens acima;

4.6.7.1.12. A atuação dos profissionais especialistas com perfil de “Implementação” deverá abranger as seguintes atividades, realizadas de acordo com o tipo de serviço demandado:

- a) Avaliar requisitos tecnológicos, definir arquitetura e projeto de infraestrutura para a construção de soluções;
- b) Definir o modelo lógico e físico de estruturas da camada de servidores de aplicação, de nomenclaturas e de sistemas de segurança;
- c) Levantar informações junto às equipes de TI do CONTRATANTE, objetivando auxiliar a definição e elaboração de aplicações/sistemas;
- d) Definir metodologia, elaborar relatórios e projetos e acompanhar a configuração e utilização de solução de alta disponibilidade, orientando sobre as melhores práticas de uso das plataformas existentes, quanto à parametrização e configuração dos componentes e ferramentas utilizadas;
- e) Elaborar projetos e acompanhar sua implantação, configuração e utilização de virtualização, com a criação e o gerenciamento de máquinas virtuais;
- f) Elaboração de documentação técnica e de usuário;
- g) Definir procedimentos de instalação e configuração das soluções nos servidores e nas estações de trabalho dos usuários administradores;
- h) Transferência de conhecimentos relacionados ao desenvolvimento, implantação e manutenção de aplicações da solução ADC;
- i) Esclarecer dúvidas e orientar sobre a utilização e a integração das soluções implantadas, abrangendo as diversas plataformas existentes no ambiente;
- j) Realizar operação assistida e monitoramento de ambientes integrados com a solução ADC;

- k) Manutenção dos sistemas pós-implantação para a verificação e correção de possíveis erros de parametrização e para otimização do funcionamento da solução ADC;
- l) Analisar o funcionamento das ferramentas instaladas e realizar alterações no ambiente, para garantir a melhor utilização e aproveitamento dos recursos oferecidos;
- m) Promover melhorias no desempenho (*tuning*), disponibilidade e confiabilidade dos ambientes;
- n) Apoiar na melhoria dos controles e do monitoramento do ambiente, sugerindo métricas, *thresholds* e indicadores de acompanhamento;
- o) Apoiar no planejamento, na execução e na avaliação das mudanças no ambiente;
- p) Apoiar a homologação de novas soluções ou de mudanças de infraestrutura, com análise do impacto no ambiente;
- q) Realizar a atualização ou instalação de novas versões de sistemas e dos produtos instalados no CONTRATANTE;
- r) Reinstalar e/ou ajustar as ferramentas em nova infraestrutura de TI;
- s) Apoiar e implementar soluções de questões referentes à utilização das ferramentas implantadas no CONTRATANTE (Linux, Red Hat, JBoss e outras plataformas);
- t) Construir novas funcionalidades e casos de uso em linguagem suportada pela solução ADC adquirida;
- u) Corrigir ou apoiar em problemas e defeitos de código identificados em funcionalidades já existentes;
- v) Condução técnica de resolução de problemas e solicitações de recursos entre a gestão de produtos do fabricante da solução e o time de engenharia (acesso direto à engenharia, sem necessidade de escalar pelos diversos níveis de suporte).

4.7. Recebimento do objeto (Art. 140, Lei n. 14.133/2021)

4.7.1. Em conformidade com o artigo 140 da Lei n.º 14.133/21, o objeto deste contrato será aceito:

4.7.1.1. Provisoriamente, pelo responsável por seu acompanhamento e fiscalização, com verificação da conformidade do material ou do serviço com as exigências contratuais, conforme cronograma do ANEXO IV;

4.7.1.2. Definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais, conforme cronograma do ANEXO IV.

4.7.2. A Equipe de Fiscalização do CONTRATANTE fará a emissão do primeiro Termo de Recebimento Provisório (TRP1), referente à etapa de fornecimento dos *appliances* que compõem a solução ADC, em até 5 (cinco) dias corridos da comunicação da CONTRATADA, conforme descrito no cronograma do ANEXO IV;

4.7.3. A CONTRATADA deverá realizar a instalação e configuração dos equipamentos e *softwares* embarcados que integram a solução, bem como a entrega das licenças de uso, no prazo máximo de 20 (vinte) dias corridos, contados a partir da data de emissão do primeiro Termo de Recebimento Provisório (TRP1) ou da Ordem de Serviço para os itens do Grupo 2, conforme cronograma constante do ANEXO IV;

4.7.4. A conclusão das etapas de instalação e configuração dos equipamentos e *softwares* embarcados da solução, bem como a entrega das licenças de uso, deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE;

4.7.5. A Equipe de Fiscalização do CONTRATANTE fará a emissão do segundo Termo de Recebimento Provisório (TRP2), referente à etapa de instalação e configuração dos equipamentos e *softwares* embarcados da solução, em até 5 (cinco) dias corridos da comunicação da CONTRATADA, conforme cronograma constante do ANEXO IV;

4.7.6. A Equipe de Fiscalização do CONTRATANTE fará a emissão do Termo de Recebimento Definitivo (TRD) da entrega, instalação, configuração e licenciamento da solução em até 10 (dez) dias corridos da emissão do segundo Termo de Recebimento Provisório (TRP2), conforme cronograma constante do ANEXO IV;

4.7.7. Na hipótese de ser verificada a inadequação do objeto com os requisitos descritos neste Termo de Referência e seus anexos no ato da entrega/execução, a equipe de fiscalização o rejeitará imediatamente, no todo ou em parte, sendo a CONTRATADA notificada a proceder à regularização no prazo máximo de 15 (quinze) dias corridos após a verificação;

4.7.7.1. Havendo reincidência quanto à impropriedade do objeto no momento da entrega/execução retificadora, poderão ser aplicadas as sanções administrativas previstas no Ajuste.

4.7.8. Após o recebimento provisório, a Equipe de Fiscalização do CONTRATANTE avaliará as características do objeto, identificando eventuais problemas;

4.7.8.1. Estando em conformidade, será efetuado o Recebimento Definitivo;

4.7.8.2. Se, após o aceite provisório, constatar-se que o objeto foi entregue em desacordo com o contrato ou com a Proposta, com incorreção, ou incompleto, serão interrompidos os prazos de recebimento e suspenso o pagamento após a notificação à CONTRATADA, condição que será mantida até o saneamento da situação.

4.7.9. Quando houver entrega de bem ou material em desacordo com o especificado neste Termo de Referência, no Instrumento Convocatório ou no contrato, bem como bem ou material que apresente defeito, será rejeitado parcial ou totalmente, conforme o caso, e a CONTRATADA será obrigada a substituí-los em 3 (três) dias, sob pena de se considerar atraso na entrega;

4.7.9.1. A CONTRATADA ficará obrigada a trocar, a suas expensas, o bem ou material que vier a ser recusado;

4.7.9.2. A CONTRATADA deverá retirar o bem ou material recusado no momento da entrega do bem ou material correto. O CONTRATANTE não se responsabilizará por qualquer dano ou prejuízo que venha a ocorrer após esse prazo;

4.7.9.3. Será considerado abandonado o bem ou material que não for recolhido pela CONTRATADA em até 30 (trinta) dias após a comunicação do CONTRATANTE;

4.7.9.4. A Administração poderá dar a destinação que julgar conveniente ao bem ou material abandonado em suas dependências;

4.7.9.5. A CONTRATADA deverá entregar todo o bem ou material discriminados nas Ordens de Serviço, não havendo pagamento em caso de entrega parcial até que ocorra o adimplemento da obrigação.

4.7.10. Independentemente da aceitação, a CONTRATADA garantirá a qualidade do serviço ou bem fornecido pelo prazo estabelecido contratualmente, obrigando-se a reparar aquele que apresentar incorreções ou defeito no prazo estabelecido pelo CONTRATANTE;

4.7.11. O aceite provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos por lei ou pelo contrato;

4.7.12. A entrega do objeto pela CONTRATADA e seu recebimento pelo CONTRATANTE não implicam sua aceitação definitiva, que será caracterizada pelo ateste da nota fiscal/fatura correspondente;

4.7.13. Eventual pedido de prorrogação dos prazos estipulados deverá ser encaminhado ao CONTRATANTE, preferencialmente, na forma eletrônica;

4.7.14. Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério do CONTRATANTE.

4.7.15. Para fins de recebimento e aceite do serviço de suporte técnico mensal serão observados os seguintes prazos:

4.7.15.1. A CONTRADA deverá emitir, ao final de cada período mensal, relatório detalhado constando a relação consolidada de chamados técnicos registrados e encaminhá-lo ao CONTRATANTE em até 5 (cinco) dias úteis contados do encerramento de cada período;

4.7.15.2. A Equipe de Fiscalização do CONTRATANTE fará, mensalmente, o Recebimento Provisório do serviço prestado, mediante a entrega do relatório detalhado de chamados técnicos, em até 3 (três) dias úteis contados da ciência da relação consolidada dos chamados abertos no mês;

4.7.15.3. A Equipe de Fiscalização do CONTRATANTE fará a emissão do Termo de Recebimento Definitivo, mediante Termo Circunstanciado, referente ao período mensal de prestação do serviço de suporte técnico, em até 7 (sete) dias úteis após a emissão do Termo de Recebimento Provisório aludido no item anterior;

4.8. Critérios de medição e pagamento (Art. 6º, XXIII, "g", Lei n. 14.133/2021)

4.8.1. A CONTRATADA deverá emitir Notas Fiscais/Faturas relativas ao fornecimento dos *appliances* que compõem a solução ADC, bem como dos serviços de instalação e configuração após receber cópia assinada do Termo de Recebimento Definitivo previsto no ANEXO IV;

4.8.2 Os pagamentos serão efetuados, por ordem bancária, mediante a apresentação de Nota Fiscal no portal SIGEO correspondente ao serviço executado (definido em cada Ordem de Serviço) e aceite definitivamente, devidamente atestada pela equipe de fiscalização do contrato, devendo ser emitida obrigatoriamente pelo CNPJ da CONTRATADA.

4.8.3. As notas fiscais deverão ser encaminhadas aos *e-mails* indicados pelo gestor do contrato ou peticionadas no sistema SEI:

a) CJF: sutec@cjf.jus.br, sti@cjf.jus.br

b) TRF3: diac@trf3.jus.br; ract@trf3.jus.br

c) JFSP: admisp-cetec@trf3.jus.br

d) JFMS: acom@trf3.jus.br

e) TRF5: sti.secretaria@trf5.jus.br

f) JFPE: atendimento@jfpe.jus.br

g) JFCE: atendimento.nti@jfce.jus.br

h) JFPB: atendimentoonti@jfpb.jus.br

i) JFAL: nti@jfal.jus.br

j) JFSE: ntic.atendimento@jfse.jus.br

k) JFRN: planejamento.dti@jfrn.jus.br

l) TRF6: secti@trf6.jus.br

4.8.4. No corpo da nota fiscal deverá ser especificado o objeto contratado, o período faturado no formato dia/mês/ano, os quantitativos dos itens, quando couber, e a identificação da respectiva nota de empenho;

4.8.5. Após recebida a nota fiscal, o Gestor do Contrato deverá atestá-la em até 5 (cinco) dias úteis e encaminhá-la à área financeira para:

4.8.5.1. liquidação da despesa, a contar do recebimento da nota fiscal, no prazo de:

a) 5 (cinco) dias úteis, nos casos dos valores que não ultrapassem o limite de que trata o inciso II do art. 75 da Lei n. 14.133/2021;

b) 10 (dez) dias úteis, nos demais casos.

4.8.5.2. pagamento da despesa, a contar da liquidação da despesa, no prazo de:

a) 5 (cinco) dias úteis, nos casos dos valores que não ultrapassem o limite de que trata o inciso II do art. 75 da Lei n. 14.133/2021;

b) 10 (dez) dias úteis, nos demais casos.

4.8.6. Os prazos de que trata o item 4.8.6.1, poderão ser excepcionalmente prorrogados, justificadamente, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais;

4.8.7. O prazo para a solução, pela CONTRATADA, de inconsistências na execução do objeto ou de saneamento da nota fiscal, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins de que trata o item 4.8.6.1;

4.8.8. Na hipótese de caso fortuito ou força maior que impeça a liquidação ou o pagamento da despesa, o prazo para o pagamento será suspenso até a sua regularização, devendo ser mantida a posição da ordem cronológica em que a despesa originalmente estava inscrita;

4.8.9. A fim de que o CONTRATANTE possa efetuar o pagamento, a CONTRATADA deverá apresentar nota fiscal constando a indicação do banco, da agência e do número da conta corrente onde deverá ser efetuado o crédito;

4.8.10. O CONTRATANTE, no momento do pagamento, providenciará as devidas retenções tributárias, nos termos da legislação vigente, exceto nos casos em que a CONTRATADA comprovar, na forma prevista em lei, não lhe serem aplicáveis tais retenções;

4.8.11. Em caso de eventual atraso de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, o valor faturado será atualizado monetariamente pelo percentual “*pro rata temporis*” do Índice de Preço ao Consumidor Amplo - IPCA conhecido quando do faturamento, compreendido entre a data limite estipulado para pagamento e aquela em que se der o efetivo pagamento.

4.9. Adequação Orçamentária (Art. 6º, XXIII, "j", Lei n. 14.133/2021)

4.9.1. A despesa em questão está prevista no Plano de Contratações Anual – PCA 2024 do Conselho da Justiça Federal (item 93) e na previsão orçamentária do exercício de 2024, sob a natureza de despesa detalhada conforme a seguir:

a) 44.90.52.43 - Equipamentos de TIC;

b) 33.90.40.22 - Instalação de Equipamentos de TI

c) 33.90.40.07 - Manutenção Corretiva/Adaptativa e Sustentação de Softwares (suporte técnico); e

d) 33.90.40.20 - Treinamento/Capacitação em TIC.

4.10. Glosas

4.10.1. O não atendimento dos Níveis Mínimos de Serviço, descritos no item 4.6.5, referentes a aferição da qualidade do serviço de suporte técnico mensal, independentemente das Sanções Administrativas previstas no contrato, implicará em redutor sobre o valor mensal do serviço de suporte técnico (glosa), nos seguintes casos:

4.10.1.1. Glosa de 20% (vinte por cento), calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso no início do atendimento dos chamados com severidade ALTA, limitada até 02 (duas) horas de atraso, a partir desse prazo será aplicada a glosa por atraso na resolução do chamado;

4.10.1.2. Glosa de 5,0% (cinco por cento), calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso no início do atendimento dos chamados com severidade MÉDIA, limitada até 6 (cinco) horas de atraso, a partir desse prazo será aplicada a glosa por atraso na resolução do chamado;

4.10.1.3. Glosa de 1,0% (um por cento), calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso no início do atendimento dos chamados com severidade BAIXA, limitada até 24 (vinte e quatro) horas de atraso, a partir desse prazo será aplicada a glosa por atraso na resolução do chamado;

4.10.1.4. Glosa de 8% (oito por cento), calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, pela não resolução dos chamados com severidade ALTA, limitada até 5 (cinco) horas de atraso;

4.10.1.5. Glosa de 3,0% (três por cento), calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, pela não resolução dos chamados com severidade MÉDIA, limitada até 10 (dez) horas de atraso;

4.10.1.6. Glosa de 1,0% (um por cento), calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, pela não resolução dos chamados com severidade BAIXA, limitada até 24 (vinte e quatro) horas de atraso.

4.10.2. Nos casos em que os atrasos forem superiores aos limites previstos nos subitens anteriores, além da aplicação das glosas supracitadas, a CONTRATADA estará sujeita às sanções administrativas citadas no item 4.11 deste Termo de Referência;

4.10.4. A aplicação da glosa servirá ainda como indicador de desempenho da CONTRATADA na execução dos serviços;

4.10.5. O faturamento do serviço de suporte técnico deverá ser mensal, mediante apresentação de nota de cobrança consolidada para todos os equipamentos e *softwares* da solução, já descontadas as glosas eventualmente aplicadas em função do não atendimento dos níveis de qualidade definidos no contrato, determinando o valor total do serviço para o mês;

4.10.6. No caso de aplicação de glosa referente à demora na conclusão de chamados do mesmo nível de severidade, para qualquer componente da solução, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 meses, será aplicada a sanção administrativa prevista no item 4.11.1.3, alínea *a*.

4.10.7. No caso de discordância das glosas aplicadas, a CONTRATADA deverá apresentar o recurso que será analisado pela Área Administrativa.

4.10.8. Se a decisão da Administração for favorável ao recurso da CONTRATADA, será emitida nota de cobrança adicional para que seja efetuado o pagamento referente ao valor glosado.

4.10.9. A nota de cobrança emitida pela CONTRATADA deverá ser atestada pelo Gestor do Contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada da documentação comprobatória das glosas.

4.11. Sanções (Art. 156, Lei n. 14133/2021)

4.11.1. No caso de atraso injustificado ou inexecução total ou parcial do compromisso assumido com o CONTRATANTE, as sanções administrativas aplicadas à CONTRATADA serão:

4.11.1.1. **Advertência** por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para o CONTRATANTE, não interfiram diretamente na execução do objeto e não comprometam prazos e/ou serviços;

4.11.1.2. Multas, nos seguintes termos:

a) Multa moratória no percentual correspondente a 0,05% (cinco centésimos por cento), calculada sobre o valor total da contratação, por dia de atraso na entrega do Plano de Implantação ou da apresentação do Preposto, do Gerente de Projetos ou do Responsável Técnico, além do prazo máximo definido no ANEXO IV - CRONOGRAMA DE IMPLANTAÇÃO, até o limite de 30 (trinta) dias corridos, a partir do qual poderá ficar caracterizada a INEXECUÇÃO PARCIAL do Contrato;

b) Multa moratória no percentual correspondente a 0,10% (um décimo por cento), calculada sobre o valor total da contratação, por dia de atraso na entrega de todos os equipamentos, *softwares* e quaisquer outros acessórios necessários para a solução, além do prazo máximo definido no ANEXO IV - CRONOGRAMA DE IMPLANTAÇÃO, até o limite de 30 (trinta) dias corridos, a partir do qual poderá ficar caracterizada a INEXECUÇÃO TOTAL do Contrato;

c) Multa moratória no percentual correspondente a 3,0% (três por cento), calculada sobre o valor total do serviço de instalação, configuração e integração da solução ADC fornecida (item 1.2 do objeto desta contratação), por dia de atraso na conclusão da etapa de instalação e configuração da solução, além dos prazos máximos definidos no ANEXO IV - CRONOGRAMA DE IMPLANTAÇÃO até o limite de 30 (trinta) dias corridos, a partir do qual poderá ficar caracterizada a INEXECUÇÃO TOTAL do Contrato.

d) Multa moratória no percentual correspondente a 2% (dois por cento), calculada sobre o valor individual do serviço do serviço de treinamento online, por dia de atraso no início ou na conclusão do serviço de transferência de conhecimento, além dos prazos máximos definidos nos itens 4.6.6.5 e 4.6.6.6, até o limite de 30 (trinta) dias corridos. Caso seja atingido qualquer um dos limites estabelecidos para o serviço de transferência de conhecimento, incidirá, a título compensatório,

60% (sessenta por cento) calculado sobre o valor total do respectivo serviço;

e) Multa moratória no percentual correspondente a 0,2% (dois décimos por cento), por dia de atraso, até o limite de 30 (trinta) dias corridos, calculada sobre o valor da garantia contratual, no caso de atraso injustificado na sua entrega, nos termos do item 4.15 - Garantia contratual. Caso seja atingido o limite estabelecido para apresentação da garantia contratual, a título compensatório, incidirão 15% (quinze por cento) sobre o valor total da garantia contratual;

f) Multa moratória no percentual correspondente a 0,10% (um décimo por cento), calculada sobre o valor total da contratação, por dia de atraso no caso de descumprimento das obrigações referentes a reparação de falhas de funcionamento ou substituição dos componentes da solução, previstas no serviço de garantia do objeto, até o limite de 30 (trinta) dias corridos, a partir do qual poderá ficar caracterizada a INEXECUÇÃO TOTAL do Contrato.

g) Multa moratória de 0,006% (seis milésimos por cento), calculada sobre o valor total da contratação, para cada hora/dia de atraso, no cumprimento de quaisquer obrigações previstas em contrato e não arroladas acima.

h) Multa compensatória de 20% (vinte por cento), quando ocorrer glosa referente a atraso no início do atendimento dos chamados do serviço de suporte com a mesma severidade por 3 (três) meses consecutivos ou 5 (cinco) meses intercalados dentro de um período de 12 (doze) meses contados a partir da primeira ocorrência. Após o limite de 1 (uma) ocorrência, durante a vigência do Contrato, será considerada INEXECUÇÃO PARCIAL.

i) Multa moratória de 1% (um por cento), calculada sobre o valor anual do serviço de suporte técnico, quando não houver resolução de chamados, dentro do prazo previsto de execução e do limitador de horas previsto nas glosas. Após o limite de 30 dias, será considerada INEXECUÇÃO PARCIAL.

4.11.1.3. Multas compensatória de:

a) 30% (trinta por cento) sobre o valor do Contrato, em caso de INEXECUÇÃO TOTAL das obrigações deste instrumento;

b) 10% (dez por cento) sobre o valor do saldo remanescente do Contrato, em caso de INEXECUÇÃO PARCIAL das obrigações deste instrumento.

c) 10% (dez por cento) sobre o valor do saldo remanescente do Contrato, em caso de não manutenção das condições de habilitação da CONTRATADA, caso em que poderá ser caracterizada a INEXECUÇÃO PARCIAL das obrigações deste instrumento.

d) O valor da multa compensatória não poderá ser inferior a 0,5% do valor total do contrato, conforme previsto no art. 156, § 3º, da Lei 14.133/2021.

4.11.1.4. Impedimento de licitar e contratar com a Administração pelo prazo de até 2 (dois) anos, quando não se justificar a imposição de penalidade mais grave;

4.11.1.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

4.11.2. A inexecução total ou parcial do contrato poderá acarretar a sua rescisão, conforme previsto neste instrumento e no art. 115 da Lei nº 14.133/2021, bem como a incidência das consequências legais cabíveis, inclusive indenização por perdas e danos, eventualmente causados ao CONTRATANTE.

4.11.3. A não manutenção das condições de habilitação da CONTRATADA ao longo da execução do contrato poderá ensejar a RESCISÃO CONTRATUAL UNILATERAL pelo Conselho da Justiça Federal após regular procedimento administrativo, resguardado à CONTRATADA o direito ao contraditório e à ampla defesa, e ainda a aplicação de multa de 10% (dez por cento) sobre o valor da contratação.

4.11.4. O valor da multa, aplicada após regular processo administrativo, seguirá a seguinte ordem de execução:

a) Descontado dos pagamentos devidos pelo CONTRATANTE à CONTRATADA; ou

b) Executado da Garantia Contratual; ou

c) Recolhido pela contratada mediante pagamento de GRU; ou

d) Cobrado Judicialmente.

4.11.5. O disposto nos itens anteriores não prejudicará a aplicação de outras penalidades a que esteja sujeita a CONTRATADA, nos termos da Lei n. 14.133/2021.

4.11.6. As penalidades serão obrigatoriamente registradas no SICAF e sua aplicação será precedida da concessão da oportunidade de ampla defesa para o adjudicatário, na forma da lei.

4.11.7. Eventual pedido de prorrogação deverá ser encaminhado ao CJF preferencialmente na forma eletrônica.

4.11.8. Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados,

e a aceitação da justificativa ficará a critério do CONTRATANTE.

4.11.19 Recursos – Da aplicação das penalidades previstas nos subitens 4.11.1.2, **4.11.1.3** e das glosas previstas na cláusula 4.10, poderão ser interpostos recursos no prazo máximo de 5 (cinco) dias úteis, a contar da intimação do ato, nos termos da Lei n. 14.133/2021.

4.11.20 Pedido de Reconsideração – No caso da penalidade prevista no subitem 4.11.1.1, caberá pedido de reconsideração à autoridade competente, no prazo de 3 (três) dias úteis a contar da intimação do ato, nos termos da Lei n. 14.133/2021.

4.12. Garantia do objeto

4.12.1. O prazo de garantia dos *appliances* físicos (item 1.1 do objeto) e direito a atualização de todos os *softwares* que compõem a solução é de 60 (sessenta) meses, contados a partir da emissão do Termo de Recebimento Definitivo (TRD) referente aos serviços de entrega, instalação e configuração da solução;

4.12.2. Para os *appliances* virtuais (itens 2.1 e 2.2 do objeto), o licenciamento/subscrições de todos os *softwares* que compõem a solução deverão vigor pelo período de 5 (cinco) anos, constados a partir da emissão do Termo de Recebimento Definitivo (TRD) referente aos serviços de entrega, instalação e configuração da solução;

4.12.2. Todos os equipamentos e/ou *softwares* que compõem a solução deverão suportar e serem fornecidos com a última versão de *firmware* disponibilizada pelo fabricante da solução durante toda a vigência do contrato;

4.12.3. Caso algum equipamento e/ou *software* da solução conste em lista de *end-of-support*, *end-of-engineering-support* ou *end-of-life* do fabricante, durante o período de vigência do contrato, a CONTRATADA deverá fornecer, configurar e promover a substituição por novo equivalente, que atenda as especificações técnicas descritas neste Termo e que não impacte na perda de funcionalidade da solução, em até 30 (dias) após a publicação da lista em site oficial do fabricante;

4.12.4. Os custos relativos à garantia dos equipamentos e do licenciamento/subscrições dos *softwares* que compõem a solução já devem estar incluídos no preço dos próprios itens;

4.12.5. O serviço de garantia técnica da solução consiste em reparar eventuais falhas de funcionamento dos equipamentos ou dos *softwares*, bem como na integração entre os componentes da solução, mediante a substituição de equipamentos e de versões dos *softwares* ou revisão de configurações, de acordo com as recomendações dos fabricantes, informações presentes nas páginas e manuais de suporte e normas técnicas específicas, nos prazos definidos no item 4.6.5 - Níveis mínimos de serviço;

4.12.6. O direito a atualização dos *softwares* obriga a CONTRATADA a disponibilizar a atualização dos *softwares* fornecidos e que compõem a solução tão logo ocorra o lançamento de novos *softwares* em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos *softwares* fornecidos;

4.12.7. A reparação de falhas de funcionamento dos componentes da solução deverá ocorrer de acordo com os seguintes princípios detalhados nos itens a seguir, acerca da garantia dos equipamentos, dos *softwares* e da integração entre os componentes que compõem a solução.

4.12.8. Quanto aos equipamentos da solução:

4.12.8.1. Dispor de estoque de peças e equipamentos de reposição, visando à prestação dos serviços de reparação do funcionamento dos equipamentos durante todo o período de garantia;

4.12.8.2. Substituir, no prazo de 24 (vinte e quatro) horas, partes e componentes dos equipamentos que apresentem defeito por outras de características idênticas ou superiores, originais e novas;

4.12.8.3. Nos casos em que não seja possível o reparo dentro do prazo estipulado no item anterior, substituir no prazo máximo de 72 (setenta e duas) horas, em caráter temporário ou definitivo, o equipamento defeituoso por outro de mesma marca e modelo, ou superior, aos adquiridos pelo Contratante e com as mesmas características técnicas, novo e de primeiro uso;

4.12.8.4. Substituir qualquer equipamento, componente ou periférico, no prazo de 120 (cento e vinte) horas, por outro original e novo, caso seja verificado que, no período de 15 (quinze) dias corridos, contados após a abertura de chamado de suporte técnico, ocorreram defeitos recorrentes que não permitam seu correto funcionamento, mesmo tendo havido substituição de partes e componentes;

4.12.8.5. Em todas as hipóteses de substituição previstas anteriormente, caso exista a impossibilidade técnica de substituição por modelo igual, novo e original, será permitida a substituição por outro com características técnicas idênticas ou superiores, plenamente compatível, também original e novo;

4.12.8.6. Devolver, em perfeito estado de funcionamento, no prazo máximo de 15 (quinze) dias corridos, a contar da data de retirada dos equipamentos, os equipamentos que necessitem ser temporariamente retirados para reparo, ficando a remoção, o transporte e a substituição sob inteira responsabilidade da CONTRATADA;

4.12.8.7. A Contratada deverá responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores de seu quadro de pessoal, assim como pelos efeitos delas advindos na execução das atividades previstas neste Termo de Referência ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por estes executadas;

4.12.8.8. Comunicar, por escrito, ao CONTRATANTE, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os equipamentos objeto deste Termo de Referência, fazendo constar a causa de inadequação e a ação devida para a correção

4.12.9. Quanto aos softwares da solução:

4.12.9.1. A CONTRATADA deverá promover o isolamento, identificação e caracterização de falhas nos *softwares* da solução consideradas “bug de software”;

4.12.9.2. Será considerado pelo CONTRATANTE como “bug de software” o comportamento ou característica dos *softwares* que se mostre diferentes daquele previsto na documentação do produto e seja considerado como prejudicial ao correto uso;

4.12.9.3. Será de exclusiva responsabilidade da CONTRATADA o encaminhamento da falha de *software* ao laboratório do fabricante, o acompanhamento da solução e a aplicação do respectivo *fix*, *patch* ou pacote de correção em dia e horário a ser definido pelo CONTRATANTE;

4.12.9.4. Responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores do quadro da empresa, assim como pelos efeitos delas advindos na execução das atividades previstas neste Termo de Referência ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por estes executadas;

4.12.9.5. Comunicar, por escrito, ao CONTRATANTE, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os softwares objeto deste Termo de Referência, fazendo constar a causa de inadequação e a ação devida para a correção;

4.12.10. Quanto a integração dos componentes da solução:

4.12.10.1. A CONTRATADA deverá manter, durante a vigência da garantia, a correta integração entre os elementos de *hardware* e *software* que compõem a solução, nas mesmas condições de desempenho e confiabilidade que apresentavam no momento de emissão do Termo de Recebimento Definitivo (TRD);

4.12.10.2. Quando forem identificadas falhas de funcionamento na solução que não sejam atribuídas diretamente aos elementos de *hardware* ou de *software*, caberá à CONTRATADA a análise e o encaminhamento da solução, buscando restaurar o correto funcionamento do conjunto de elementos da solução;

4.12.10.3. Serão consideradas como falhas de funcionamento da integração dos componentes a redução significativa do desempenho ou a perda de funcionalidades técnicas disponibilizadas pelo conjunto da solução;

4.12.10.4. A atualização dos *softwares* fornecidos que compõem a solução, deverá ocorrer de acordo com os seguintes princípios:

- a) O CONTRATANTE deverá ter direito irrestrito, durante a vigência da garantia, de atualizar as versões de todos os *softwares* que compõem a solução, mesmo que os fabricantes alterem suas políticas de licenciamento dos softwares;
- b) O direito a atualização de versões dos *softwares* que compõem a solução não poderá gerar qualquer custo adicional para o CONTRATANTE;
- c) Deverão ser criadas contas de acesso, em nome do CONTRATANTE, no site de suporte do fabricante dos *softwares* que compõem a solução, na mesma data do início da prestação dos serviços demandados na Ordem de Serviço inicial;
- d) O perfil das contas criadas em nome do CONTRATANTE deverá permitir de forma irrestrita o download de *drivers*, *firmwares*, *patches*, atualizações, novas versões, informações de suporte, acesso a base de conhecimento e manuais técnicos;
- e) Sempre que solicitado, mediante chamado de Suporte Técnico, a CONTRATADA deverá orientar o CONTRATANTE quanto aos procedimentos técnicos para a instalação ou atualização de versões dos *softwares* que compõem a solução.

4.13. Local da execução contratual

4.13.1. A entrega do objeto constante da Ordem de Serviço será realizada nas dependências do respectivo CONTRATANTE, em dias úteis em que houver expediente, das 8:00 às 16:00 horas.

4.13.2. A entrega dos equipamentos, *softwares* e qualquer acessório que componha o objeto, bem como a realização dos

serviços de garantia e suporte previstos neste contrato deverão ser realizados na sede do CONTRATANTE, conforme relação abaixo:

- a) Conselho da Justiça Federal – CJF: Setor de Almoxarifado, localizado no Setor de Clubes Esportivos Sul Trecho 3 – Polo 8 – Lote 9 – Brasília - DF, CEP: 70200-003;
- b) Superior Tribunal de Justiça – STJ: situado no SAFS, St. de Administração Federal Sul Quadra 06, Lote 01, Trecho III – Brasília - DF, CEP: 70095-900;
- c) Tribunal Regional Federal da 3ª Região – TRF3: situado na Av. Paulista, 1842 – Bela Vista, São Paulo - SP, CEP: 01310-936;
- d) Seção Judiciária de Mato Grosso do Sul: R. Delegado Carlos Roberto Bastos de Oliveira, 128 - Parque dos Poderes, Campo Grande - MS, 79037-102d) Fórum Ministro Pedro Lessa: situado na Av. Paulista, 1682 - Bela Vista, São Paulo - SP, CEP: 01310-200;
- e) Tribunal Regional Federal da 6ª Região – TRF6: situado na Av. Álvares Cabral, nº 1.805, 5º andar, Bairro Santo Agostinho, Belo Horizonte - MG, CEP: 30.170-008;
- f) Tribunal Regional Federal da 5ª Região – TRF5: A CONTRATADA deverá consultar cada site das seções judiciárias da Justiça Federal da 5ª Região no momento da contratação. A entrega do licenciamento/subscrições poderá ser realizada por *e-mail*, visto que se trata de solução virtual.

4.14. Informações acerca da análise/ impacto ambiental decorrente da contratação

4.14.1. A CONTRATADA será responsabilizada por qualquer prejuízo que venha causar ao CJF em virtude de ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ligadas aos produtos e serviços objeto do presente Termo de Referência.

4.14.2. A CONTRATADA deverá, para a execução dos serviços, fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços, conforme disposto no art. 6º, inciso IV, da Instrução Normativa SLTI/MPOG n. 01, de 19 de janeiro de 2010;

4.14.3. A CONTRATADA deverá comprovar que bens ofertados atendem aos critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos no art. 3º, II, do Decreto n. 7.174, de 12 de maio de 2010 e pela Portaria INMETRO n. 170, de 10 de abril de 2012.

4.14.4. A comprovação do item anterior, quando solicitada pela Administração, poderá ser feita mediante apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, ou ainda por qualquer outro meio de prova, inclusive declaração voluntária, que ateste que os bens fornecidos cumprem com as exigências, conforme o art. 42, I e III, da Lei n. 14.133, de 1º de abril de 2021.

4.14.5. A CONTRATADA deverá observar, sempre que possível, para a entrega dos produtos adquiridos, as normas em vigor atinentes à sustentabilidade e ao Manual de Sustentabilidade nas compras e contratações do Conselho da Justiça Federal, instituído pela Portaria CJF n. 96, de 10 de fevereiro de 2023.

4.14.6. A CONTRATADA deverá respeitar a legislação vigente e as normas técnicas elaboradas pela ABNT e pelo INMETRO para aferição e garantia de aplicação dos requisitos mínimos de qualidade e segurança dos produtos adquiridos neste Termo de Referência.

4.15. Garantia contratual (Art. 96, Lei n. 14.133/2021)

4.15.1. Para o Grupo 1, a CONTRATADA se compromete a apresentar garantia para assegurar o fiel cumprimento das obrigações assumidas, no percentual de 5% (cinco por cento) do valor anual do Contrato, em até 20 (vinte) dias úteis contados da assinatura do contrato por parte da CONTRATANTE, nas modalidades de garantia previstas nos incisos I e III do art. 96, §1º da Lei n. 14.133/2021.

4.15.1.1 Já para o Grupo 2, a CONTRATADA se compromete a apresentar garantia para assegurar o fiel cumprimento das obrigações assumidas, no percentual de 5% (cinco por cento) do valor total do Contrato, em até 20 (vinte) dias úteis contados da assinatura do contrato por parte da CONTRATANTE, nas modalidades de garantia previstas nos incisos I e III do art. 96, §1º da Lei n. 14.133/2021.

4.15.2 No caso de a CONTRATADA optar pela constituição de seguro-garantia, deverá apresentar a cautela, no prazo de 1 (um) mês, contado da data de homologação da licitação, nos termos do § 3º do art. 96 da Lei 14.133/2021.

4.15.3 Quando a garantia for apresentada na modalidade seguro-garantia, a apólice deverá ser expedida exclusivamente por qualquer das entidades controladas e fiscalizadas pela Superintendência de Seguros Privados (SUSEP). Deverá ser apresentado o número com que a apólice ou o endosso tenha sido registrado na SUSEP.

4.15.4 Será permitida a substituição da apólice na data de renovação ou de aniversário do contrato, desde que mantidas as mesmas condições e coberturas da apólice vigente e desde que nenhum período fique descoberto, ressalvado o que dispõe o §2º do art. 96 da NLLC.

4.15.5 Quando a garantia for apresentada em dinheiro, ela será atualizada monetariamente, conforme os critérios estabelecidos pela instituição bancária em que for realizado o depósito., nos termos do art. 100 da Lei n. 14.133/2021.

4.15.6 Caso a CONTRATADA opte pela modalidade fiança bancária, o instrumento respectivo deverá ser expedido exclusivamente por qualquer das entidades controladas e fiscalizadas pelo Banco Central do Brasil. Além disso, a pessoa fiadora deverá ser domiciliada ou possuir agência no Distrito Federal e demonstrar possuir bens suficientes à garantia integral da fiança prestada, conforme art. 825 da Lei 10.406/2002. A carta de fiança deverá conter cláusula 10.406/2002, conforme facultado pelo inciso I do artigo 828 do mesmo diploma legal, e ser registrada no Registro de Títulos e Documentos, conforme previsto nos artigos 128, 129 e 130 da Lei 6.015/73.

4.15.7 Aditado o Contrato ou alterado o seu valor, fica a CONTRATADA obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e modalidades constantes deste Termo de Referência, em até 20 (vinte) dias úteis, contados da assinatura do instrumento ou do início da nova vigência contratual. Nesses casos, a garantia será liberada após a apresentação da nova garantia e da assinatura do Termo Aditivo ao Contrato.

4.15.8 A garantia apresentada em desacordo com os requisitos e coberturas previstos será devolvida à CONTRATADA, que disporá do prazo adicional improrrogável de 10 (dez) dias corridos para a regularização da pendência, sem prejuízo da aplicação da penalidade cabível.

4.15.9. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

- a) prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
- b) prejuízos causados à Administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;
- c) multas moratórias e punitivas aplicadas pela Administração à CONTRATADA;
- d) obrigações e ações trabalhistas, previdenciárias e para com o FGTS e sua respectiva multa, não adimplidas pela CONTRATADA, quando couber.

4.15.10. Para efeitos da execução da garantia, os inadimplementos contratuais deverão ser comunicados pelo CONTRATANTE à CONTRATADA e/ou à Instituição Garantidora, no prazo máximo de 90 (noventa) dias após o término de vigência do contrato.

4.17. Confidencialidade de informações (Art. 32, § 2º, Lei n. 14.133/2021)

4.17.1. A CONTRATADA compromete-se a manter em caráter confidencial, mesmo após a eventual rescisão do contrato, todas as informações a seguir especificadas:

4.17.1.1. Política de segurança adotada pelo CJF e pelos órgãos da Justiça Federal e as configurações de *hardware* e *software* relacionadas.

4.17.1.2. Processo de instalação, configuração e customizações de produtos, ferramentas e os itens constantes do(s) objeto(s).

4.17.1.3. Qualquer informação do CONTRATANTE que venha tomar conhecimento em razão da execução dos serviços.

4.17.2. A CONTRATADA deverá concordar e assinar Termo de Confidencialidade e Sigilo da Contratada especificado no ANEXO VI.

5. Equipe de Planejamento da Contratação - EPC

5.1 O presente Termo de Referência foi elaborado pela Equipe de Planejamento da Contratação, nomeada por intermédio da Portaria CJF n. 377/2025 (id. 0736096), identificada adiante:

Integrante		Nome	Matrícula
Demandante	Titular	JEFFERSON COLOMBO BARBOSA XAVIER	740
	Suplente	ADRIANA JESUS DE MORAIS	382
Técnico	Titular	GABRIEL OLIVEIRA MENEZES	1150
	Suplente	NÉLIO ALVES DA SILVA	999
Administrativo	Titular	GERALDO COSTA CAVALCANTE	1106
	Suplente	PAULO VITOR CAIXETA FERRAZ	1027

ANEXO I – DETALHAMENTO DOS REQUISITOS TÉCNICOS DO OBJETO PARA O GRUPO 1

1. DOS REQUISITOS GERAIS

1.1. Modelo de referência: F5 Big-IP R4800 com Premium Service e Best Bundle, subscrição de IP Intelligence e Threat Campaigns.(serão aceitas soluções de mesma marca e modelo ou de similares compatíveis e de qualidade superior, para que seja assegurada compatibilidade com a solução em uso no STJ).

1.2. A solução é composta por 2 (dois) equipamentos do tipo ADC (Application Delivery Controller) com funções de Web Application Firewall (WAF), incluindo o fornecimento de transceivers, serviços de instalação, configuração, transferência de conhecimento, garantia e suporte técnico;

1.3. O licenciamento de software do ADC deverá ser de uso perpétuo, exceto para funcionalidades relacionadas a atualizações periódicas de suas bases de inteligência que deverão ter seu funcionamento garantido até a expiração das licenças (vigência contratual). Dessa maneira, as atualizações de versões do ADC, o acesso à base de inteligência, bem como seu suporte e garantia serão interrompidos. Não obstante, as funcionalidades que não dependerem de atualizações periódicas deverão continuar funcionando plenamente.

1.4. Os equipamentos devem ser novos, de primeiro uso e estar em linha de fabricação na data de entrega da solução.

1.5. Devem possuir homologação da Agência Nacional de Telecomunicações (ANATEL) com validade indeterminada, conforme determina a Resolução nº 715, de 23 de outubro de 2019.

1.6. Os hardwares e softwares ofertados na composição dos itens não devem estar listados como "End of Sale" e "End of Life" por seus respectivos fabricantes até a data da abertura das propostas.

1.6.1. Durante a período da garantia, a CONTRATADA deverá manter todas as condições previstas em edital até o término da vigência contratual, devendo, inclusive, atualizar a solução integralmente por equipamentos compatíveis (com as especificações exigidas e com o equipamento originalmente ofertado), sem ônus adicional ao CONTRATANTE, caso a descontinuidade da solução se dê durante o o período de garantia.

1.7. As versões de software dos equipamentos fornecidos devem ser disponibilizadas de forma global por seus fabricantes, com acesso amplo por parte da base de clientes, não sendo aceitas versões de software desenvolvidas de forma customizada para atendimento ao presente certame.

1.8. A partir do lançamento de uma atualização de software, os processos de mudança de versão podem ser especificados, controlados e executados pelo próprio cliente, com ou sem o apoio da CONTRATADA, sem prejuízo ao suporte às funcionalidades existentes;

1.9. Para atendimento do Inciso III, Art. 3º do Decreto 7.174/2010, quando da entrega dos equipamentos, o licitante deverá comprovar a origem dos bens importados e apresentar comprovante de quitação dos tributos de importação a eles referentes, sob pena de suspensão do(s) pagamento(s), rescisão contratual e multa.

1.10. Por questões de compatibilidade, gerência, suporte e garantia, os equipamentos descritos neste anexo deverão ser de um mesmo fabricante, salvo disposto em contrário.

1.11. A solução deverá incluir quaisquer equipamentos e/ou componentes necessários ao pleno funcionamento e acomodação física, ambiental e lógica no ambiente do contratante, em conformidade com os padrões estabelecidos pelo fabricante.

1.12. Os equipamentos (hardware) deverão ser montados em bastidores (racks) de 19 (dezenove) polegadas (padrão EIA-310-D) e vir acompanhados de todos os acessórios para permitir essa montagem.

1.13. A solução deve possuir memória RAM mínima de 64 GB.

1.14. Deve possuir disco SSD com capacidade de armazenamento interno e retenção de logs para análise de no mínimo 480 GB.

1.15. Deve possuir fontes de alimentação redundantes AC bivolt com as seguintes características:

1.15.1. Internas ao equipamento;

1.15.2. Com ajuste automático de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).

1.15.3. Possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos.

1.15.4. Ser capaz de sustentar a carga de todo o equipamento com todas as portas ativas, com apenas umas das fontes instalada.

1.15.5. Ser capaz de realizar a troca da fonte redundante com o equipamento em pleno funcionamento, sem nenhum impacto na performance (hot-swappable).

1.15.6. Vir acompanhadas com cabos de energia elétrica em conformidade com o padrão NBR14.136.

1.15.7. Permitir operação normal em temperaturas de 0°C até 40°C e umidade relativa de 5% a 85% (sem condensação);

1.16. Deve possuir ventiladores redundantes;

1.17. Cada equipamento deve possuir, no mínimo, 04 (quatro) portas 10 Gigabit Ethernet compatíveis com padrão RJ 45.

1.18. Cada equipamento deve possuir, no mínimo, 04 (quatro) portas 25 Gigabit Ethernet compatíveis com transceivers SFP+ ou SFP28.

1.19. Cada equipamento deve ser fornecido com os seguintes transceivers e cabos:

1.19.1. 04 (quatro) transceivers SFP+ SR (velocidade 10 Gbps) ou 04 (quatro) transceivers SFP28-SR (velocidade 25 Gbps), conforme o critério do CONTRATANTE, para fibras multimodo com conectores do tipo LC duplex, incluindo o fornecimento dos cordões ópticos (OM4, no mínimo), com comprimento mínimo de 2,5m;

1.20. Deve possuir, no mínimo, 01 (uma) porta de gerenciamento Ethernet 10/100/1000BASE-T, com conectores RJ-45. Esta porta será conectada na rede de gerência, permitindo a configuração de endereço IP próprio para gerenciamento. Deve permitir o acesso para gerenciamento do equipamento pelas demais portas.

1.21. Deve ser possível configurar 02 (duas) das portas 10 Gigabit Ethernet para sincronização de heartbeat;

1.22. Deve possuir recursos de agregação de portas baseado no protocolo LACP em seus modos ativo e passivo;

1.23. Deve funcionar sob a forma de cluster composto por dois appliances físicos.

1.24. O cluster deve operar tanto no modo ativo/passivo quanto no modo ativo/ativo;

2. DA CAPACIDADE E DESEMPENHO

2.1. Deve suportar, no mínimo, 40 (quarenta) Gbps de throughput em camada 7 e 50 (cinquenta) Gbps em camada 4 do modelo OSI;

2.2. Deve suportar, no mínimo, 30 (trinta) Gbps de compressão em hardware para tráfego HTTP;

2.3. Deve suportar, no mínimo, 1.800.000 (um milhão e oitocentos mil) requisições por segundo na camada 7 do modelo OSI;

2.4. Deve suportar, no mínimo, 750.000 (setecentos e cinquenta mil) conexões por segundo na camada 4 do modelo OSI;

2.5. Deve suportar, no mínimo, 38.000.000 (trinta e oito milhões) de conexões simultâneas na camada 4 do modelo OSI;

2.6. Deve processar, no mínimo, 20.000 (vinte mil) transações SSL/TLS por segundo usando hardware especializado;

3. DAS FUNCIONALIDADES

3.1. Deve possuir suporte a SNMPv3;

3.2. Deve permitir autenticação em bases remotas por LDAP;

3.3. Deve possuir três níveis de usuários de administração da solução: super usuário, usuário com permissões reduzidas e usuário com direito exclusivo a leitura;

3.4. Deve ter a opção de armazenamento de registros de sistema (log) na solução ou em servidores externos;

3.5. Dever possuir interface gráfica com usuário GUI (Graphic User Interface) acessível via navegador web e em conformidade com os padrões W3C, com acesso e operação por HTTPS por qualquer ponto da rede TCP/IP interna do contratante, que permita operação da solução e transferência de arquivos entre a solução e a máquina onde houve o acesso à GUI de maneira criptografada;

3.6. Deve possuir interface de linhas de comandos CLI (Command Line Interface) acessível e operável via SSH por qualquer ponto da rede TCP/IP interna, que permita operação da solução e transferência de arquivos entre a solução e sistemas externos de maneira criptografada;

3.7. Deve ter a capacidade de reinicialização remota da solução por GUI e/ou CLI;

3.8. Deve ter a capacidade de aplicar atualizações preventivas, corretivas e de melhoria através da GUI e/ou CLI;

3.9. Deve possuir suporte à linguagem de programação ou interface (API) para automatização de atividades e configurações de sistemas, sem custo adicional;

3.10. Deve ser disponibilizada documentação das APIs dos appliances que compõem a solução;

3.11. Deve ser transparente quanto ao uso do protocolo IPv4 e IPv6 para a criação, modificação, remoção ou qualquer interação com equipamentos e servidores, reais ou virtuais;

3.12. Deve permitir o redirecionamento de páginas de erros 403, 404 e 50x específicas para páginas definidas pelo administrador;

3.13. Deve permitir que a solicitação de autenticação do cliente seja configurada conforme métodos abaixo:

3.13.1. Por certificado digital, enviando as informações do certificado (ex.: CN, DN) à aplicação de destino por header ou cookie específico.

3.13.2. Por formulário, verificando as credenciais via LDAP;

3.14. Deve ser capaz de limitar o número de sessões estabelecidas com cada servidor real e virtual.

3.15. Deve implementar Listas de Controle de Acesso (ACL), utilizando, no mínimo, os parâmetros de endereço IP de origem e destino.

3.16. Deve oferecer proteção contra ataques de negação de serviço - Denial of Service (DoS) e Distributed Denial of Service (DDoS).

3.17. Deve implementar limpeza de cabeçalho HTTP.

3.18. Deve possuir registro de logs com pelo menos as seguintes características:

3.18.1. Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;

3.18.2. Os registros de log de acesso e eventos devem ser armazenados em arquivo ou banco de dados que permita a exportação ou em outro formato aberto 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;

3.18.3. Permitir configurar a retenção dos logs por tempo e ou volume.

3.19. Deve conter a funcionalidade de cache integrado, que tem por objetivo armazenar as respostas no cache interno para aliviar a carga de consumo de banda dos servidores.

3.20. Deve possuir suporte a Virtual Extensible LAN (VXLAN).

3.21. Deve se integrar com sistemas de gerenciamento de containers (ex.: Kubernetes/Openshift), de modo a permitir que mudanças dinâmicas na infraestrutura de microsserviços sejam refletidas automaticamente no balanceamento de entrada, aumentando ou diminuindo a quantidade de pods, e ainda, inserindo ou removendo serviços do Big-IP.

3.22. Deve ser integrado nativamente ao Kubernetes/Openshift para realizar o balanceamento entre pods.

3.23. Deve criar os serviços de Balanceamento de Carga dinamicamente ao mesmo tempo em que uma nova aplicação é provisionada pelo Kubernetes/Openshift.

4. DO BALANCEAMENTO LOCAL E GLOBAL

4.1. Não deve utilizar agentes ou qualquer outro tipo de aplicação instalada nos servidores ou clientes para executar suas funções e gerenciamento.

4.2. Deve ser capaz de balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação.

4.3. Deve possuir, no mínimo, capacidade de resposta aos clientes por roteamento direto (os servidores balanceados respondem diretamente aos clientes), tunelamento (a solução é capaz de utilizar servidores de redes diferentes da que está inserida) ou full Proxy (todas as transações entre clientes e servidores são intermediadas pela solução).

4.4. Deve possuir, no mínimo, capacidade de balancear pelo menos 32 (trinta e dois) servidores virtuais por agrupamento (pool) vinculados a um VIP.

4.5. Deve ser capaz de operar com os seguintes algoritmos de balanceamento:

4.5.1. Fila circular simples (Round Robin - RR);

4.5.2. Fila circular ponderada (Weighted RR - WRR);

4.5.3. Menos conexões (Least Connections);

4.5.4. Servidor com resposta mais rápida;

4.5.5. Dinâmico, baseado em parâmetros do servidor coletados via SNMP.

4.5.6. Deve ser capaz de monitorar servidores reais e virtuais pelos seguintes métodos:

4.5.6.1. Portas TCP e UDP;

4.5.6.2. ICMP;

4.5.6.3. Conexões específicas de aplicação HTTP, HTTPS, FTP, RADIUS, SMTP, LDAP (em especial, Microsoft AD), POP3, SIP, SNMP. Caso a solução apresentada não possua algum desses monitores pré-configurados ("built in"), admite-se sua criação customizada durante a fase de instalação.

4.5.7. Mesmo com a criação de novas sessões, deve garantir a persistência de sessões existentes entre clientes e servidores:

- 4.5.7.1. por análise da URL acessada;
- 4.5.7.2. por análise de qualquer parâmetro no cabeçalho (header) HTTP;
- 4.5.7.3. por cookie - inserção de um novo cookie na sessão;
- 4.5.7.4. por cookie - utilização do valor do cookie da aplicação, sem adição de cookie;
- 4.5.7.5. por sessão SSL;
- 4.5.7.6. por endereço IP destino;
- 4.5.7.7. por endereço IP origem;
- 4.5.7.8. por análise do SIP Call ID.
- 4.5.8. Deve oferecer funcionalidades de otimização, cache proxy e compressão HTTP, com capacidade de:
 - 4.5.8.1. Comprimir conteúdos HTTP (com o intuito de reduzir a quantidade de informações enviadas ao cliente);
 - 4.5.8.2. Possibilitar uso de compressão de dados com formato GZIP;
 - 4.5.8.3. Suportar a utilização e ajuste manual de quantidade memória RAM como cache proxy de objetos HTTP, para responder às requisições dos clientes sem utilizar recursos dos servidores;
 - 4.5.8.4. Permitir a reescrita de requisições HTTP baseado no conteúdo da URL, possibilitando o redirecionamento de requisições HTTP para HTTPS;
 - 4.5.8.5. Permitir a definição de quais tipos de objeto serão armazenados ou não em cache;
 - 4.5.8.6. Permitir a reescrita de respostas HTTP, possibilitando a inclusão de cabeçalho (header) customizado;
 - 4.5.8.7. Suportar multiplexação TCP e Reuso de Sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados;
 - 4.5.8.8. Suportar os protocolos HTTP, HTTP/1.1 e HTTP/2.0.
 - 4.5.8.9. Utilizar cache em memória RAM para maior velocidade no tempo de resposta;
- 4.5.9. Deve suportar, no mínimo, as seguintes métricas para política de Balanceamento Global (GSLB):
 - 4.5.9.1. Última resposta;
 - 4.5.9.2. Status de saúde;
 - 4.5.9.3. Número de servidores ativos em cada site;
 - 4.5.9.4. Geolocalização;
 - 4.5.9.5. Round Robin;
 - 4.5.9.6. Número de sessões;
 - 4.5.9.7. Connection Load do site;
 - 4.5.9.8. Disponibilidade Global.
- 4.5.10. Deve suportar a realização de GSLB de forma transparente nos demais sites, desde que seja do mesmo fabricante e suportar mecanismos de visando Disaster Recovery e redundância entre Data Centers por meio de Route Health Injection (RHI).
- 4.5.11. Deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário.
- 4.5.12. Deve servir às respostas as requisições onde o DNS é o autoritativo a partir da memória RAM; para este item, poderá ser aceita declaração do fabricante que comprove a funcionalidade.
- 4.5.13. Deve possuir proteções contra ataques DNS, no mínimo:
 - 4.5.13.1. Pacotes malformados;
 - 4.5.13.2. Inspeção de Protocolo;
 - 4.5.13.3. UDP Flood;
 - 4.5.13.4. Validação de Protocolo;
 - 4.5.13.5. Ataque ICMP.
- 4.5.14. Deve ser capaz de realizar filtragem de pacotes.
- 4.5.15. Deve ser capaz de realizar IP Anycast.
- 4.5.16. Deve ser capaz de realizar balanceamento dos servidores DNS.
- 4.5.17. Deve ser capaz de realizar DNSSec, independente da estruturados servidores DNS em uso.

4.5.18. Deve possuir alta disponibilidade, independente de BGP ou outro protocolo de roteamento. A 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.

4.5.19. 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.

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

4.5.21. Deve suportar a monitoração de estado de saúde de servidores e serviços, garantindo a disponibilidade do serviço oferecido.

4.5.22. Deve operar, no mínimo, as seguintes formas:

4.5.22.1. DNSSec.

4.5.22.2. Balanceamento de DNS Servers;

4.5.22.3. DNS Autoritativo ou DNS Secundário;

4.5.23. Deve implementar persistência de conexão do usuário entre aplicações ou data centers.

4.5.24. Deve permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada.

4.5.25. Deve permitir que a contingência seja automática, mas que o retorno seja manual.

4.5.26. Deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6).

5. DOS REQUISITOS DE SEGURANÇA

5.1. Deve possuir as funcionalidades:

5.1.1. Deve ser independente de softwares proprietários (agentes) para a execução de quaisquer funções especificadas, bem como operar em alta disponibilidade independentemente de qualquer protocolo de roteamento.

5.1.2. Deve, no mínimo, permitir a criação de novas regras com parâmetros e expressões regulares definidos pelo administrador.

5.1.3. Deve, no mínimo, permitir a criação de políticas diferenciadas por aplicação.

5.1.4. Deve, no mínimo, permitir 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.

5.1.5. Deve, no mínimo, permitir a detecção e bloqueio de ataques a aplicação Web dos tipos abaixo:

5.1.5.1. SQL, Cookie e Command Injection;

5.1.5.2. Code Injection;

5.1.5.3. Violações do protocolo HTTP;

5.1.5.4. Ameaças Web AJAX/JSON;

5.1.5.5. Cross-Site Scripting (XSS);

5.1.5.6. Cross-Site Request Forgery;

5.1.5.7. Buffer Overflow;

5.1.5.8. XML bombs/DoS;

5.1.5.9. Força bruta no browser;

5.1.5.10. Manipulação de campos escondidos e manipulação de cookies;

5.1.5.11. Cookie poisoning;

5.1.5.12. Sequestro de sessão;

5.1.5.13. Checagem de cabeçalho do "user-agent" para identificar clientes inválidos.

5.1.6. Deve, no mínimo, permitir a detecção e bloqueio da resposta de determinada aplicação Web nos casos abaixo:

5.1.6.1. Ausência de tratamento de erros pela aplicação;

5.1.6.2. 5.1.6.2. Vazamento de informações de infraestrutura.

5.1.7. Deve, no mínimo, permitir a customização da resposta de bloqueio.

5.1.8. Deve, no mínimo, proteger contra de ataques de força bruta em páginas de login.

5.1.9. Deve permitir o funcionamento do WAF usando o protocolo HTTP nas suas versões 1.0, 1.1 e 2 tanto do lado

cliente quanto do lado servidor.

5.1.10. Deve, no mínimo, permitir o bloqueio de métodos HTTP a critério do usuário.

5.1.11. Deve, no mínimo, permitir o bloqueio de ataques no modo blacklisting e whitelisting.

5.1.12. Deve, no mínimo, permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.

5.1.13. Deve, no mínimo, possuir funcionalidade de aprendizagem automática do funcionamento de uma aplicação web, suas URLs, parâmetros, dentre outras, para a configuração do bloqueio.

5.1.14. Deve, no mínimo, possuir funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação ou através de aprovação de regras pelo administrador.

5.1.15. Deve, no mínimo, permitir a customização, pelo administrador, dos parâmetros aprendidos, de forma a criar regras baseadas no tamanho do parâmetro, tipo de conteúdo, e expressões regulares.

5.1.16. Deve ser possível desabilitar algumas assinaturas específicas ou regras em determinados parâmetros, como uma exceção à regra geral.

5.1.17. Deve, no mínimo, funcionar como proxy reverso de aplicações, incluindo a tradução de URLs para diferentes Servidores Virtuais.

5.1.18. Deve, no mínimo, permitir o mapeamento de diversas aplicações em um mesmo IP virtual, enviando informações para conjuntos de servidores diferentes de acordo com a URL requisitada.

5.1.19. Deve, no mínimo, permitir o mapeamento em um mesmo IP virtual, de acordo com a URL requisitada, que exija certificado digital de cliente para algumas aplicações e não exija para outras.

5.1.20. Deve, no mínimo, permitir a configuração do modo para somente de detecção ou bloqueio, globalmente ou por cada regra.

5.1.21. Deve, no mínimo, permitir a aplicação de novas regras sem interromper as conexões já abertas.

5.1.22. Deve, no mínimo, permitir a inclusão do IP do cliente no campo X-Forwarded-For.

5.1.23. Deve, no mínimo, permitir a inclusão de parâmetros customizados nos cabeçalhos (headers) HTTP, além da alteração dos existentes, para envio à aplicação de destino.

5.1.24. Deve, no mínimo, ter suporte a SNI (Server Name Indication).

5.1.25. Deve, no mínimo, permitir no mínimo 32 servidores virtuais por grupamento (pool) vinculados a cada endereço IP virtual (VIP).

5.1.26. Deve, no mínimo, permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.

5.1.27. Deve, no mínimo, implementar proteção ao JSON (JavaScriptObject Notation).

5.1.28. Deve, no mínimo, permitir a geração de relatórios customizados do módulo de Web Application Firewall, disponibilizando no mínimo os relatórios abaixo:

5.1.28.1. URL e endereços IPs.

5.1.28.2. Top Ataques (geral ou por aplicação/servidor);

5.1.28.3. Tipos de Ataques;

5.1.28.4. Severidade;

5.1.28.5. Violações;

5.1.28.6. Países;

5.1.28.7. Top IPs de origem dos ataques;

5.1.28.8. Estatística de Tráfego;

5.1.29. Deve, no mínimo, permitir o agendamento e envio por e-mail dos relatórios, essa funcionalidade pode ser executada no equipamento ou pelo software de gerência.

5.1.30. Deve, no mínimo, permitir exportar os relatórios nos formatos HTML ou PDF.

5.1.31. Deve realizar a reputação de endereços IP, através de serviço de assinatura com atualização frequente online durante o período da garantia, impedindo que aplicações internas sejam acessadas por endereços IP maliciosos, botnets e proxys anônimos;

5.1.32. A solução deve ser capaz de criar filtros de endereços IPs baseados em reputação, com no mínimo as seguintes categorias: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing, Proxy;

- 5.1.33.** Deve aplicar os filtros de reputação considerando o endereço IP e o cabeçalho HTTP X-Forwarded-For;
- 5.1.34.** Deve realizar a reputação de endereços IP, permitindo a configuração de whitelist para permitir a liberação de acessos considerados legítimos e de baixo risco;
- 5.1.35.** Deve realizar proteção contra ataques automatizados, incluindo botnets, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma não operada por humanos;
- 5.1.36.** Deve realizar a identificação e bloqueio contra ataques sofisticados sem impactar nas transações das aplicações para os protocolos HTTP e HTTPS;
- 5.1.37.** Deve realizar a identificação de ataques, contendo nome, campo atacado, quantidade de ataques, horário e endereços IPs envolvidos, através de relatórios históricos;
- 5.1.38.** Deve identificar campanhas de ameaças usando base de conhecimento dinâmica e atualizada do fabricante para ameaças dinâmicas visando ataques de dia-zero.
- 5.1.39.** Deve possibilitar a correlação entre um incidente de ataque singular como parte de uma campanha de ameaça mais complexa e sofisticada.
- 5.1.40.** Para cada campanha identificada, deve informar no mínimo o nível de risco da campanha, o tipo de ataque, o endereço IP interno e qual VIP onde foram identificados atividade relacionada à ameaça.
- 5.1.41.** Deve ser capaz de verificar listas de endereços de alto risco cibernético, frequentemente atualizadas, e prover inteligência de contexto analisando as requisições para identificar fontes de ameaças.
- 5.1.42.** Deve realizar a identificação de dados sensíveis em páginas WEB, tais como senhas de acesso, por meio de campos de formulário, e o mascaramento, de forma a ocultar essa informação nos logs gerados;
- 5.1.43.** Deve suportar criptografia de dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação.
- 5.1.44.** Deve proteger o login e as credenciais dos usuários e com isso os dados da aplicação com criptografia.
- 5.1.45.** Deve possuir uma proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque.
- 5.1.46.** Deve ser possível proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário.
- 5.1.47.** Deve ser possível proteger esses dados criptografados de malwares e keyloggers.
- 5.1.48.** Deve ser possível identificar anomalias e mitigá-las, através da análise contínua de carga e monitoração de saúde de servidores.
- 5.2.** Deve suportar as funcionalidades de segurança para proteção DDoS:
- 5.2.1.** Suportar proteção contra todos os tipos de ataques Denial of Service (DoS e DDoS);
- 5.2.2.** Proteger de ataques DDoS que utilizem SSL;
- 5.2.3.** 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.
- 5.2.4.** Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.
- 5.2.5.** Permitir proteção contra ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.
- 5.2.6.** Permitir proteger contra ataques de DNS DDoS utilizando mecanismo que bloqueie somente as requisições maliciosas e permita requisições legítimas aos domínios existentes.
- 5.2.7.** Suportar Network Address Translation (NAT);
- 5.2.8.** Limitar o número de conexões;
- 5.2.9.** Suportar Listas de Controle de Acesso (ACL);
- 5.2.10.** Permitir o log de ataques do tipo DoS;
- 5.2.11.** Possuir ferramenta flexível baseado em linguagem de programação open-source para customizar e aumentar o nível de segurança contra ataques DDoS, incluindo a possibilidade de interação com base de reputação de endereços IP e estatísticas de tráfego.
- 5.2.12.** Suportar relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DoS e DDoS.
- 5.2.12.1.** Os relatórios devem indicar, no mínimo, a aplicação sendo atacada, o número de transações por aplicação e a latência da aplicação.

5.2.13. Possuir suporte ao envio de SNMP traps para cada ataque DDoS detectado.

5.2.14. Possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes com atributos específicos através da solução anti-DoS.

5.2.15. Ser possível a configuração do sistema para detectar e mitigar assinaturas dinâmicas. Quando configurado o sistema deve detectar possíveis ameaças DoS baseado no histórico do tráfego e poderá automaticamente mitigar essas ameaças.

5.3. Deve fornecer acesso seguro as aplicações:

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

5.3.2. Deve ser capaz de realizar Single Sign On utilizando KERBEROS;

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

5.3.4. 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);

5.3.5. Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware;

5.3.6. Deve ser capaz de autenticar usuários em bases de dados LDAP, RADIUS, TACACS+, ou Active Directory;

5.3.7. Deve possuir o modo onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitido outro tipo de tráfego dentro do mesmo túnel;

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

5.3.9. Deve possuir o modo onde um usuário se conecta efetivamente a` rede interna, obtendo um endereço IP roteável pela rede interna;

5.3.10. Deve possuir Suporte a compressão HTTP;

5.3.11. Deve possuir suporte a split tunneling;

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

5.3.13. Deve permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento DTLS (Datagram TLS);

5.3.14. Deve possibilitar compressão de dados antes de sua criptografia;

5.3.15. Deve possibilitar utilização de área de trabalho protegida, onde os arquivos de trabalho devem ser criptografados e, ao fim de cada sessão, removidos automaticamente para garantir o máximo nível de segurança;

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

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

6. DO TRATAMENTO DE TRÁFEGO SSL

6.1. Deve permitir a encriptação/decriptação de sessões SSL no lugar dos servidores (processo conhecido como SSL Offload);

6.2. Deve permitir que a terminação SSL/Troca de chaves/criptografia seja feita com aceleração em hardware;

6.3. Deve possibilitar encriptação até o servidor real;

6.4. Deve permitir que requisições HTTPS possam ser enviadas diretamente aos servidores por meio de protocolo HTTP aberto;

6.5. Deve possuir políticas de controle de acesso e autenticação baseadas nos atributos de certificado;

6.6. Deve permitir que o WAF "recriptografe" (em SSL/TLS, utilizando um certificado interno privado diferente do certificado válido) as requisições do cliente para o servidor real, antes destas serem para ele enviadas. Deve ser possível configurar um algoritmo e tamanho de chave distinto do utilizado no estabelecimento do túnel criptografado entre o cliente e o WAF;

6.7. Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados assistida por hardware especializado.

6.7.1. Permitir recriptografar a conexão entre a solução e o servidor;

6.7.2. Permitir espelhamento de tráfego de conexões TLS;

6.7.3. Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2 (SHA256/384) e Chacha20-Poly1305;

6.8. Em relação ao tráfego TLS, deve suportar:

6.8.1. Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;

6.8.2. Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;

6.8.3. Autenticação mútua (mTLS), quando ambas as autenticações acima mencionadas ocorrendo de forma simultânea;

6.8.4. Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;

6.8.5. Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente;

6.8.6. Se autenticar com o servidor utilizando um certificado de cliente, próprio da solução, com os mesmos atributos do certificado do cliente;

6.9. As listas de acesso devem ser baseadas nos atributos de um certificado.

6.10. Deve permitir ações caso o certificado original do servidor não seja confiável ou esteja expirado;

6.11. Deve permitir "by-pass" do tráfego caso o TLS handshake falhe;

6.12. Deve permitir a verificação da validade do certificado digital apresentado:

6.12.1. Pelo cliente através de Listas de Certificados Revogados (LCR) ou através de listas;

6.12.2. Via OCSP (Online Certificate Status Protocol);

6.13. Deve usar sempre o último arquivo LCR para a consulta de Lista de Certificados Revogados;

6.14. Deve implementar os protocolos TLS versões 1.1, 1.2 e 1.3;

6.15. Deve manter e gerenciar todo o tráfego criptografado com protocolo, TLS versões 1.1, 1.2 e 1.3;

6.16. Deve implementar o algoritmo de hash SHA1;

6.17. Deve implementar renegociação de sessão;

6.18. Deve possuir os seguintes algoritmos de encriptação: 3DES, RSA, AES128 e AES-256, ECCDHE (P-256 e P-384) e algoritmo de autenticação ECDSA;

6.19. Deve permitir geração de chaves RSA, enrollment de certificado, importação e exportação de chaves, certificados de servidores, e checagem de LCR (Lista de Certificados Revogados);

6.20. Por direcionamento inteligente de tráfego SSL entende-se a capacidade de abrir o tráfego SSL de entrada ("INBOUND") encaminhá-lo, de forma seletiva, levando em conta o contexto de serviço, às diferentes soluções de segurança que estão no ambiente de Data Center. No âmbito deste projeto serão exigidas, no mínimo, as integrações com as soluções de NG Firewall.

6.21. Deve suportar pelo menos as seguintes cifras e protocolos: TLS 1.1, 1.2 e 1.3, SHA, SHA2, AES-GCM, AES;

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

6.23. Deve terminar as conexões SSL com a finalidade de inspecioná-las.

6.24. Deve proteger de ataques de negação de serviço que utilizem SSL.

6.25. Deve ser possível descobrir ameaças ocultas no SSL/TLS e prevenir ataques em vários estágios, usando as soluções de segurança já existentes assim como novas soluções que venham a ser adquiridas futuramente, independente de marca/modelo.

6.26. Deve ter capacidade de gerenciar o tráfego SSL do lado do cliente para o servidor, ou seja, deve ser capaz de decifrar todo o tráfego de entrada.

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

6.28. Deve suportar SSL Forward Secrecy como uma forma de melhorar a segurança nas transações SSL/TLS. Deve ser capaz de criar múltiplos Service Chains.

6.29. Deve suportar a renegociação de sessão;

6.30. Deve possibilitar a monitoração e gerenciamento independente de cada dispositivo da cadeia de inspeção. Deve possuir um mecanismo de classificação contextual do tráfego que será enviado para cada dispositivo.

6.31. Deve fazer a monitoração dos serviços dentro da camada de inspeção

6.32. Deve permitir a resiliência dos serviços dentro da zona de inspeção, inclusive fazendo o balanceamento de carga entre múltiplos equipamentos do mesmo serviço.

6.33. Deve permitir escalar os dispositivos de segurança com alta disponibilidade, usando testes de monitoração de saúde para identificar o estado de cada equipamento de segurança.

6.34. Deve ser possível prevenir ameaças de entrada (Data Center) e de saída (usuários), incluindo ataques de exploração, retorno de chamada e extração de dados.

7. DO GERENCIAMENTO LOCAL

7.1. Deve possuir funcionalidade de emissão de relatório gerencial/estatístico dos acessos em ferramenta local ou remota, além do syslog ou log interno, que contenham, no mínimo

7.1.1. Quantidade de acessos por VIP;

7.1.2. Possuir MIB SNMP.

7.1.3. Quantidade de acessos por serviços e servidores;

7.1.4. Quantidade de usuários conectados;

7.1.5. Disponibilidade dos serviços/VIP;

7.1.6. Tempo de latência do cliente e servidor;

7.1.7. Throughput de requisição e resposta;

7.1.8. Transações por segundo;

7.1.9. Quantidade de requisições por período;

7.1.10. Quantidade de sessões;

7.1.11. Retenção de logs para análise posterior;

7.2. Deve ser disponibilizada documentação das APIs dos appliances que compõem a solução;

7.3. Deve ser capaz de analisar a performance de aplicações web.

7.4. Deve gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, troubleshooting, planejamento de capacidade e análise da experiência dos usuários finais no acesso às aplicações.

7.5. Deve, a partir das informações coletadas, permitir a análise dos dados por aplicações, por URLs, por clientes e por servidores, permitindo, assim, a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução.

7.6. Deve gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados. Caso a solução não possua este recurso nativamente poderá ser aceita solução de terceiros para atendimento da especificação.

7.7. Deve permitir o detalhamento do tempo de resposta total de carregamento de uma URL/página.

7.8. Deve suportar mecanismos para criar usuários com no mínimo três conjuntos distintos de privilégios, sendo um deles somente leitura das configurações, para acesso às funções de gerenciamento dos equipamentos, via protocolos SSH, SNMP ou HTTPS.

7.9. Deve possibilitar a coleta de dados de gerenciamento dos equipamentos utilizando os protocolos SNMPv2c e SNMPv3.

7.10. Deve suportar MIB SNMP.
7.11. Deve permitir a configuração de endereços IPs para o envio de traps SNMP (alarmes).

ANEXO II – DETALHAMENTO DOS REQUISITOS TÉCNICOS DO OBJETO PARA O GRUPO 2

Appliance Virtual Tipo 1 (uma unidade virtual – licenciamento/subscrições para 5 anos)

- 1 x F5-BIG-VE-BTA-1G-V18 (BIG-IP VIRTUAL EDITION: BEST BUNDLE 1 GBPS (V12.1.X V18.X))
- 2 x F5-SBS-BIGVE-IPI21YR (BIG-IP Subscription: IP Intelligence License **1YR** (VE-1G/VE-3G/VE-5G))
- 1 x F5-SBS-BIGVE-IPI23YR (BIG-IP Subscription: IP Intelligence License **3YR** (VE-1G/VE-3G/VE-5G))
- 2 x F5-SBS-BIG-VE-TC21YR (BIG-IP Subscription: Adv WAF Threat Campaigns License for VE **1YR** (VE-1G))
- 1 x F5-SBS-BIG-VE-TC23YR (BIG-IP Subscription: Adv WAF Threat Campaigns License for VE **3YR** (VE-1G))

1. Características de desempenho e escalabilidade da unidade básica da solução:

- 1.1 Possuir capacidade mínima para tratar 1 Gbps de throughput;
- 1.2 Suportar, no mínimo 2 vCPU em cada appliance;
- 1.3 Deve suportar a configuração de, no mínimo, 04 (quatro) GB de memória RAM;
- 1.4 Deve ser compatível com sistemas de virtualização VMware EXi 7 ou superior;
- 1.5 Suportar 802.1q para o transporte de múltiplas VLAN por uma única porta e por um conjunto agregado de portas;
- 1.6 A solução deve permanecer plenamente operante após o fim da garantia contratada, sem interrupção de tráfego ou funcionalidades, sendo admitido apenas o encerramento dos serviços de atualização de assinaturas e bases de inteligência;
- 1.7 Os equipamentos desta solução devem ser appliances virtuais do mesmo fabricante, modelo, versão e licenciamento, sendo essa exigência requisito técnico fundamental para configuração de dispositivos que operarão em modo cluster;

Appliance Virtual Tipo 2 (uma unidade virtual - licenciamento/subscrições para 5 anos)

- 1 x F5-BIG-VE-BTA-10G-V18 (BIGIP VIRTUAL EDITION: BEST BUNDLE 10 GBPS (V12.1.X V18.X))
- 2 x F5-SBS-BIGVE-IP131YR (BIG-IP Subscription: IP Intelligence License **1YR** (VE-10G))
- 1 x F5-SBS-BIGVE-IP133YR (BIG-IP Subscription: IP Intelligence License **3YR** (VE-10G))
- 2 x F5-SBS-BIG-VE-TC31YR (BIG-IP Subscription: Adv WAF Threat Campaigns License for VE **1YR** (3G/High Performance VE))
- 1 x F5-SBS-BIG-VE-TC33YR (BIG-IP Subscription: Adv WAF Threat Campaigns License for VE **3YR** (3G/High Performance VE))

1. Características de desempenho e escalabilidade da unidade básica da solução:

- 1.1 Possuir capacidade mínima para tratar 9 Gbps de throughput;
- 1.2 Suportar, no mínimo 8 vCPU em cada appliance;
- 1.3 Deve suportar a configuração de, no mínimo, 16 (dezesesseis) GB de memória RAM;
- 1.4 Deve ser compatível com sistemas de virtualização VMware EXi 7 ou superior;
- 1.5 Suportar 802.1q para o transporte de múltiplas VLAN por uma única porta e por um conjunto agregado de portas;
- 1.6 A solução deve permanecer plenamente operante após o fim da garantia contratada, sem interrupção de tráfego ou funcionalidades, sendo admitido apenas o encerramento dos serviços de atualização de assinaturas e bases de inteligência;
- 1.7 Os equipamentos desta solução devem ser appliances virtuais do mesmo fabricante, modelo, versão e licenciamento, sendo essa exigência requisito técnico fundamental para configuração de dispositivos que operarão em modo cluster;

CARACTERÍSTICAS COMUNS PARA O TIPO 1 E TIPO 2

1 DOS REQUISITOS GERAIS

1.1 A solução é composta por 1 (um) appliance virtual do tipo ADC (Application Delivery Controller) com funções de Web Application Firewall (WAF), serviços de instalação, configuração, transferência de conhecimento, garantia e suporte técnico;

1.2 O licenciamento de software do ADC deverá ser de uso perpétuo, exceto para funcionalidades relacionadas a atualizações periódicas de suas bases de inteligência que deverão ter seu funcionamento garantido até a expiração das licenças (vigência contratual). Dessa maneira, as atualizações de versões do ADC/WAF, o acesso à base de inteligência, bem como seu suporte e garantia serão interrompidos. Não obstante, as funcionalidades que não dependerem de atualizações periódicas deverão continuar funcionando plenamente.

1.3 A composição dos itens não deve estar listados como "End of Sale" e "End of Life" por seus respectivos fabricantes até a data da abertura das propostas.

1.4 Durante a período da garantia, a CONTRATADA deverá manter todas as condições previstas em edital até o término da vigência contratual, devendo, inclusive, atualizar a solução integralmente por outra compatível (com as especificações originalmente), sem ônus adicional ao CONTRATANTE, caso a descontinuidade da solução se dê durante o período de garantia.

As versões de software dos equipamentos fornecidos devem ser disponibilizadas de forma global por seus fabricantes, com acesso amplo por parte da base de clientes, não sendo aceitas versões de software desenvolvidas de forma customizada para atendimento ao presente certame.

1.5 A partir do lançamento de uma atualização de software, os processos de mudança de versão podem ser especificados, controlados e executados pelo próprio cliente, com ou sem o apoio da CONTRATADA, sem prejuízo ao suporte às funcionalidades existentes;

1.6 Para atendimento do Inciso III, Art. 3º do Decreto 7.174/2010, quando da entrega do objeto, o licitante deverá comprovar a origem dos bens importados e apresentar comprovante de quitação dos tributos de importação a eles

referentes, sob pena de suspensão do(s) pagamento(s), rescisão contratual e multa.

1.7 Por questões de compatibilidade, gerência, suporte e garantia, os objetos descritos neste anexo deverão ser de um mesmo fabricante, salvo disposto em contrário.

1.8 A solução deverá incluir quaisquer componentes necessários ao pleno funcionamento e acomodação física, ambiental e lógica no ambiente do contratante, em conformidade com os padrões estabelecidos pelo fabricante.

1.9 Deve permitir operação em cluster tanto no modo ativo/passivo quanto no modo ativo/ativo;

2 DAS FUNCIONALIDADES

2.1 Deve possuir suporte a SNMPv3;

2.2 Deve permitir autenticação em bases remotas por LDAP;

2.3 Deve possuir três níveis de usuários de administração da solução: super usuário, usuário com permissões reduzidas e usuário com direito exclusivo a leitura;

2.4 Deve ter a opção de armazenamento de registros de sistema (log) na solução ou em servidores externos;

2.5 Dever possuir interface gráfica com usuário GUI (Graphic User Interface) acessível via navegador web e em conformidade com os padrões W3C, com acesso e operação por HTTPS por qualquer ponto da rede TCP/IP interna do contratante, que permita operação da solução e transferência de arquivos entre a solução e a máquina onde houve o acesso à GUI de maneira criptografada;

2.6 Deve possuir interface de linhas de comandos CLI (Command Line Interface) acessível e operável via SSH por qualquer ponto da rede TCP/IP interna, que permita operação da solução e transferência de arquivos entre a solução e sistemas externos de maneira criptografada;

2.7 Deve ter a capacidade de reinicialização remota da solução por GUI e/ou CLI;

2.8 Deve ter a capacidade de aplicar atualizações preventivas, corretivas e de melhoria através da GUI e/ou CLI;

2.9 Deve possuir suporte à linguagem de programação ou interface (API) para automatização de atividades e configurações de sistemas, sem custo adicional;

2.10 Deve ser disponibilizada documentação das APIs dos appliances virtuais que compõem a solução;

2.11 Deve ser transparente quanto ao uso do protocolo IPv4 e IPv6 para a criação, modificação, remoção ou qualquer interação com equipamentos e servidores, reais ou virtuais;

2.12 Deve permitir o redirecionamento de páginas de erros 403, 404 e 50x específicas para páginas definidas pelo administrador;

2.13 Deve permitir que a solicitação de autenticação do cliente seja configurada conforme métodos abaixo:

2.14 Por certificado digital, enviando as informações do certificado (ex.: CN, DN) à aplicação de destino por header ou cookie específico.

2.15 Por formulário, verificando as credenciais via LDAP;

2.16 Deve ser capaz de limitar o número de sessões estabelecidas com cada servidor real e virtual.

2.17 Deve implementar Listas de Controle de Acesso (ACL), utilizando, no mínimo, os parâmetros de endereço IP de origem e destino.

2.18 Deve oferecer proteção contra ataques de negação de serviço - Denial of Service (DoS) e Distributed Denial of Service (DDoS).

2.19 Deve implementar limpeza de cabeçalho HTTP.

2.20 Deve possuir registro de logs com pelo menos as seguintes características:

2.21 Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;

2.22 Os registros de log de acesso e eventos devem ser armazenados em arquivo ou banco de dados que permita a exportação ou em outro formato aberto 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;

2.23 Permitir configurar a retenção dos logs por tempo e ou volume.

2.24 Deve conter a funcionalidade de cache integrado, que tem por objetivo armazenar as respostas no cache interno para

aliviar a carga de consumo de banda dos servidores.

2.25 Deve possuir suporte a Virtual Extensible LAN (VXLAN).

2.26 Deve se integrar com sistemas de gerenciamento de containers (ex.: Kubernetes/OpenShift), de modo a permitir que mudanças dinâmicas na infraestrutura de microsserviços sejam refletidas automaticamente no balanceamento de entrada, aumentando ou diminuindo a quantidade de pods, e ainda, inserindo ou removendo serviços do Big-IP.

2.27 Deve ser integrado nativamente ao Kubernetes/OpenShift para realizar o balanceamento entre pods.

2.28 Deve criar os serviços de Balanceamento de Carga dinamicamente ao mesmo tempo em que uma nova aplicação é provisionada pelo Kubernetes/OpenShift.

3 DO BALANCEAMENTO LOCAL E GLOBAL

3.1 Não deve utilizar agentes ou qualquer outro tipo de aplicação instalada nos servidores ou clientes para executar suas funções e gerenciamento.

3.2 Deve ser capaz de balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação.

3.3 Deve possuir, no mínimo, capacidade de resposta aos clientes por roteamento direto (os servidores balanceados respondem diretamente aos clientes), tunelamento (a solução é capaz de utilizar servidores de redes diferentes da que está inserida) ou full Proxy (todas as transações entre clientes e servidores são intermediadas pela solução).

3.4 Deve possuir, no mínimo, capacidade de balancear pelo menos 32 (trinta e dois) servidores virtuais por agrupamento (pool) vinculados a um VIP.

3.5 Deve ser capaz de operar com os seguintes algoritmos de balanceamento:

3.5.1 Fila circular simples (Round Robin - RR);

3.5.2 Fila circular ponderada (Weighted RR - WRR);

3.5.3 Menos conexões (Least Connections);

3.5.4 Servidor com resposta mais rápida;

3.5.5 Dinâmico, baseado em parâmetros do servidor coletados via SNMP.

3.5.6 Deve ser capaz de monitorar servidores reais e virtuais pelos seguintes métodos:

3.5.7 Portas TCP e UDP;

3.5.8 ICMP;

3.5.9 Conexões específicas de aplicação HTTP, HTTPS, FTP, RADIUS, SMTP, LDAP (em especial, Microsoft AD), POP3, SIP, SNMP. Caso a solução apresentada não possua algum desses monitores pré-configurados ("built in"), admite-se sua criação customizada durante a fase de instalação.

3.6 Mesmo com a criação de novas sessões, deve garantir a persistência de sessões existentes entre clientes e servidores:

3.6.1 por análise da URL acessada;

3.6.2 por análise de qualquer parâmetro no cabeçalho (header) HTTP;

3.6.3 por cookie - inserção de um novo cookie na sessão;

3.6.4 por cookie - utilização do valor do cookie da aplicação, sem adição de cookie;

3.6.5 por sessão SSL;

3.6.6 por endereço IP destino;

3.6.7 por endereço IP origem;

3.6.8 por análise do SIP Call ID.

3.7 Deve oferecer funcionalidades de otimização, cache proxy e compressão HTTP, com capacidade de:

3.7.1 Comprimir conteúdos HTTP (com o intuito de reduzir a quantidade de informações enviadas ao cliente);

3.7.2 Possibilitar uso de compressão de dados com formato GZIP;

3.7.3 Suportar a utilização e ajuste manual de quantidade memória RAM como cache proxy de objetos HTTP, para responder às requisições dos clientes sem utilizar recursos dos servidores;

3.7.4 Permitir a reescrita de requisições HTTP baseado no conteúdo da URL, possibilitando o redirecionamento de requisições HTTP para HTTPS;

3.7.5 Permitir a definição de quais tipos de objeto serão armazenados ou não em cache;

3.7.6 Permitir a reescrita de respostas HTTP, possibilitando a inclusão de cabeçalho (header) customizado;

3.7.7 Suportar multiplexação TCP e Reuso de Sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados;

3.7.8 Suportar os protocolos HTTP, HTTP/1.1 e HTTP/2.0.

3.7.9 Utilizar cache em memória RAM para maior velocidade no tempo de resposta;

3.8 Deve suportar, no mínimo, as seguintes métricas para política de Balanceamento Global (GSLB):

3.8.1 Última resposta;

3.8.2 Status de saúde;

3.8.3 Número de servidores ativos em cada site;

3.8.4 Geolocalização;

3.8.5 Round Robin;

3.8.6 Número de sessões;

3.8.7 Connection Load do site;

3.8.8 Disponibilidade Global.

3.9 Deve suportar a realização de GSLB de forma transparente nos demais sites, desde que seja do mesmo fabricante e suportar mecanismos de visando Disaster Recovery e redundância entre Data Centers por meio de Route Health Injection (RHI).

3.10 Deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário.

3.11 Deve servir às respostas as requisições onde o DNS é o autoritativo a partir da memória RAM; para este item, poderá ser aceita declaração do fabricante que comprove a funcionalidade.

3.12 Deve possuir proteções contra ataques DNS, no mínimo:

3.12.1 Pacotes malformados;

3.12.2 Inspeção de Protocolo;

3.12.3 UDP Flood;

3.12.4 Validação de Protocolo;

3.12.5 Ataque ICMP.

3.13 Deve ser capaz de realizar filtragem de pacotes.

3.14 Deve ser capaz de realizar IP Anycast.

3.15 Deve ser capaz de realizar balanceamento dos servidores DNS.

3.16 Deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso.

3.17 Deve possuir alta disponibilidade, independente de BGP ou outro protocolo de roteamento. A 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.

3.18 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.

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

3.20 Deve suportar a monitoração de estado de saúde de servidores e serviços, garantindo a disponibilidade do serviço oferecido.

3.21 Deve operar, no mínimo, as seguintes formas:

3.22 DNSSec.

3.23 Balanceamento de DNS Servers;

- 3.24 DNS Autoritativo ou DNS Secundário;
- 3.25 Deve implementar persistência de conexão do usuário entre aplicações ou data centers.
- 3.26 Deve permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada.
- 3.27 Deve permitir que a contingência seja automática, mas que o retorno seja manual.
- 3.28 Deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6).

4 DOS REQUISITOS DE SEGURANÇA

4.1 Deve ser independente de softwares proprietários (agentes) para a execução de quaisquer funções especificadas, bem como operar em alta disponibilidade independentemente de qualquer protocolo de roteamento, quando em cluster.

4.2 Deve, no mínimo, permitir a criação de novas regras com parâmetros e expressões regulares definidos pelo administrador.

4.3 Deve, no mínimo, permitir a criação de políticas diferenciadas por aplicação.

4.4 Deve, no mínimo, permitir 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.

4.5 Deve, no mínimo, permitir a detecção e bloqueio de ataques a aplicação Web dos tipos abaixo:

4.5.1 SQL, Cookie e Command Injection;

4.5.2 Code Injection;

4.5.3 Violações do protocolo HTTP;

4.5.4 Ameaças Web AJAX/JSON;

4.5.5 Cross-Site Scripting (XSS);

4.5.6 Cross-Site Request Forgery;

4.5.7 Buffer Overflow;

4.5.8 XML bombs/DoS;

4.5.9 Força bruta no browser;

4.5.10 Manipulação de campos escondidos e manipulação de cookies;

4.5.11 Cookie poisoning;

4.5.12 Sequestro de sessão;

4.5.13 Checagem de cabeçalho do "user-agent" para identificar clientes inválidos.

4.6 Deve, no mínimo, permitir 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.

4.7 Deve, no mínimo, permitir a detecção e bloqueio de ataques a aplicações Web dos tipos abaixo:

4.7.1 SQL, Cookie e Command Injection;

4.7.2 Code Injection;

4.7.3 Violações do protocolo HTTP;

4.7.4 Ameaças Web AJAX/JSON;

4.7.5 Cross-Site Scripting (XSS);

4.7.6 Cross-Site Request Forgery;

4.7.7 Buffer Overflow;

4.7.8 XML bombs/DoS;

4.7.9 Força bruta no browser;

4.7.10 Manipulação de campos escondidos e manipulação de cookies;

4.7.11 Cookie poisoning;

- 4.7.12 Sequestro de sessão;
- 4.7.13 Checagem de cabeçalho do "user-agent" para identificar clientes inválidos.
- 4.8 Deve, no mínimo, permitir a detecção e bloqueio da resposta de determinada aplicação Web nos casos abaixo:
 - 4.8.1 Ausência de tratamento de erros pela aplicação;
 - 4.8.2 Vazamento de informações de infraestrutura.
- 4.9 Deve, no mínimo, permitir a customização da resposta de bloqueio.
- 4.10 Deve, no mínimo, proteger contra de ataques de força bruta em páginas de login.
- 4.11 Deve permitir o funcionamento do WAF usando o protocolo HTTP nas suas versões 1.0, 1.1 e 2, tanto do lado cliente quanto do lado servidor.
- 4.12 Deve, no mínimo, permitir o bloqueio de métodos HTTP a critério do usuário.
- 4.13 Deve, no mínimo, permitir o bloqueio de ataques no modo blacklisting e whitelisting.
- 4.14 Deve, no mínimo, permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.
- 4.15 Deve, no mínimo, possuir funcionalidade de aprendizagem automática do funcionamento de uma aplicação web, suas URLs, parâmetros, dentre outras, para a configuração do bloqueio.
- 4.16 Deve, no mínimo, possuir funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação ou através de aprovação de regras pelo administrador.
- 4.17 Deve, no mínimo, permitir a customização, pelo administrador, dos parâmetros aprendidos, de forma a criar regras baseadas no tamanho do parâmetro, tipo de conteúdo, e expressões regulares.
- 4.18 Deve ser possível desabilitar algumas assinaturas específicas ou regras em determinados parâmetros, como uma exceção à regra geral.
- 4.19 Deve, no mínimo, funcionar como proxy reverso de aplicações, incluindo a tradução de URLs para diferentes Servidores Virtuais.
- 4.20 Deve, no mínimo, permitir o mapeamento de diversas aplicações em um mesmo IP virtual, enviando informações para conjuntos de servidores diferentes de acordo com a URL requisitada.
- 4.21 Deve, no mínimo, permitir o mapeamento em um mesmo IP virtual, de acordo com a URL requisitada, que exija certificado digital de cliente para algumas aplicações e não exija para outras.
- 4.22 Deve, no mínimo, permitir a configuração do modo para somente de detecção ou bloqueio, globalmente ou por cada regra.
- 4.23 Deve, no mínimo, permitir a aplicação de novas regras sem interromper as conexões já abertas.
- 4.24 Deve, no mínimo, permitir a inclusão do IP do cliente no campo X-Forwarded-For.
- 4.25 Deve, no mínimo, permitir a inclusão de parâmetros customizados nos cabeçalhos (headers) HTTP, além da alteração dos existentes, para envio à aplicação de destino.
- 4.26 Deve, no mínimo, ter suporte a SNI (Server Name Indication).
- 4.27 Deve, no mínimo, permitir no mínimo 32 servidores virtuais por agrupamento (pool) vinculados a cada endereço IP virtual (VIP).
- 4.28 Deve, no mínimo, permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.
- 4.29 Deve, no mínimo, implementar proteção ao JSON (JavaScriptObject Notation).
- 4.30 Deve, no mínimo, permitir a geração de relatórios customizados do módulo de Web Application Firewall, disponibilizando no mínimo os relatórios abaixo:
 - 4.30.1 URL e endereços IPs.
 - 4.30.2 Top Ataques (geral ou por aplicação/servidor);
 - 4.30.3 Tipos de Ataques;
 - 4.30.4 Severidade;

- 4.30.5 Violações;
- 4.30.6 Países;
- 4.30.7 Top IPs de origem dos ataques;
- 4.30.8 Estatística de Tráfego;
- 4.31 Deve, no mínimo, permitir o agendamento e envio por e-mail dos relatórios, essa funcionalidade pode ser executada no equipamento ou pelo software de gerência.
- 4.32 Deve, no mínimo, permitir exportar os relatórios nos formatos HTML ou PDF.
- 4.33 Deve realizar a reputação de endereços IP, através de serviço de assinatura com atualização frequente online durante o período da garantia, impedindo que aplicações internas sejam acessadas por endereços IP maliciosos, botnets e proxys anônimos;
- 4.34 A solução deve ser capaz de criar filtros de endereços IPs baseados em reputação, com no mínimo as seguintes categorias: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing, Proxy;
- 4.35 Deve aplicar os filtros de reputação considerando o endereço IP e o cabeçalho HTTP X-Forwarded-For;
- 4.36 Deve realizar a reputação de endereços IP, permitindo a configuração de whitelist para permitir a liberação de acessos considerados legítimos e de baixo risco;
- 4.37 Deve realizar proteção contra ataques automatizados, incluindo botnets, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma não operada por humanos;
- 4.38 Deve realizar a identificação e bloqueio contra ataques sofisticados sem impactar nas transações das aplicações para os protocolos HTTP e HTTPS;
- 4.39 Deve realizar a identificação de ataques, contendo nome, campo atacado, quantidade de ataques, horário e endereços IPs envolvidos, através de relatórios históricos;
- 4.40 Deve identificar campanhas de ameaças usando base de conhecimento dinâmica e atualizada do fabricante para ameaças dinâmicas visando ataques de dia-zero.
- 4.41 Deve possibilitar a correlação entre um incidente de ataque singular como parte de uma campanha de ameaça mais complexa e sofisticada.
- 4.42 Para cada campanha identificada, deve informar no mínimo o nível de risco da campanha, o tipo de ataque, o endereço IP interno e qual VIP onde foram identificados atividade relacionada à ameaça.
- 4.43 Deve ser capaz de verificar listas de endereços de alto risco cibernético, frequentemente atualizadas, e prover inteligência de contexto analisando as requisições para identificar fontes de ameaças.
- 4.44 Deve realizar a identificação de dados sensíveis em páginas WEB, tais como senhas de acesso, por meio de campos de formulário, e o mascaramento, de forma a ocultar essa informação nos logs gerados;
- 4.45 Deve suportar criptografia de dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação.
- 4.46 Deve proteger o login e as credenciais dos usuários e com isso os dados da aplicação com criptografia.
- 4.47 Deve possuir uma proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque.
- 4.48 Deve ser possível proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário.
- 4.49 Deve ser possível proteger esses dados criptografados de malwares e keyloggers.
- 4.50 Deve ser possível identificar anomalias e mitigá-las, através da análise contínua de carga e monitoração de saúde de servidores.
- 4.51 Deve suportar as funcionalidades de segurança para proteção DDoS:
 - 4.51.1 Suportar proteção contra todos os tipos de ataques Denial of Service (DoS e DDoS);
 - 4.51.2 Proteger de ataques DDoS que utilizem SSL;
 - 4.51.3 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.
 - 4.51.4 Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.

4.51.5 Permitir proteção contra ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.

4.51.6 Permitir proteger contra ataques de DNS DDoS utilizando mecanismo que bloqueie somente as requisições maliciosas e permita requisições legítimas aos domínios existentes.

4.51.7 Suportar Network Address Translation (NAT);

4.51.8 Limitar o número de conexões;

4.51.9 Suportar Listas de Controle de Acesso (ACL);

4.51.10 Permitir o log de ataques do tipo DoS;

4.51.11 Possuir ferramenta flexível baseado em linguagem de programação open-source para customizar e aumentar o nível de segurança contra ataques DDoS, incluindo a possibilidade de interação com base de reputação de endereços IP e estatísticas de tráfego.

4.51.12 Suportar relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DoS e DDoS.

4.51.13 Os relatórios devem indicar, no mínimo, a aplicação sendo atacada, o número de transações por aplicação e a latência da aplicação.

4.51.14 Possuir suporte ao envio de SNMP traps para cada ataque DDoS detectado.

4.51.15 Possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes com atributos específicos através da solução anti-DoS.

4.51.16 Ser possível a configuração do sistema para detectar e mitigar assinaturas dinâmicas. Quando configurado o sistema deve detectar possíveis ameaças DoS baseado no histórico do tráfego e poderá automaticamente mitigar essas ameaças.

4.52 Deve fornecer acesso seguro as aplicações:

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

4.52.2 Deve ser capaz de realizar Single Sign On utilizando KERBEROS;

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

4.52.4 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);

4.52.5 Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware;

4.52.6 Deve ser capaz de autenticar usuários em bases de dados LDAP, RADIUS, TACACS+, ou Active Directory;

4.52.7 Deve possuir o modo onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitido outro tipo de tráfego dentro do mesmo túnel;

4.52.8 Deve possuir modo onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;

4.52.9 Deve possuir o modo onde um usuário se conecta efetivamente a` rede interna, obtendo um endereço IP roteável pela rede interna;

4.52.10 Deve possuir Suporte a compressão HTTP;

4.52.11 Deve possuir suporte a split tunneling;

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

4.52.13 Deve permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento DTLS (Datagram TLS);

4.52.14 Deve possibilitar de compressão de dados antes de sua criptografia;

4.52.15 Deve possibilitar utilização de área de trabalho protegida, onde os arquivos de trabalho devem ser criptografados e, ao fim de cada sessão, removidos automaticamente para garantir o máximo nível de segurança;

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

4.52.17 Deve oferecer acesso remoto seguro a` rede inteira para qualquer aplicação baseada em IP (TCP ou UDP);

5 DO TRATAMENTO DE TRÁFEGO SSL

5.1 Deve permitir a encriptação/decriptação de sessões SSL no lugar dos servidores (processo conhecido como SSL Offload);

5.2 Deve permitir que a terminação SSL/Troca de chaves/criptografia seja feita com aceleração em hardware;

5.3 Deve possibilitar encriptação até o servidor real;

5.4 Deve permitir que requisições HTTPS possam ser enviadas diretamente aos servidores por meio de protocolo HTTP aberto;

5.5 Deve possuir políticas de controle de acesso e autenticação baseadas nos atributos de certificado;

5.6 Deve permitir que o WAF "recriptografe" (em SSL/TLS, utilizando um certificado interno privado diferente do certificado válido) as requisições do cliente para o servidor real, antes destas serem para ele enviadas. Deve ser possível configurar um algoritmo e tamanho de chave distinto do utilizado no estabelecimento do túnel criptografado entre o cliente e o WAF;

5.7 Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados assistida por hardware especializado.

5.8 Permitir recriptografar a conexão entre a solução e o servidor;

5.9 Permitir espelhamento de tráfego de conexões TLS;

5.10 Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2 (SHA256/384) e Chacha20-Poly1305;

5.11 Em relação ao tráfego TLS, deve suportar:

5.11.1 Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;

5.11.2 Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;

5.11.3 Autenticação mútua (mTLS), quando ambas as autenticações acima mencionadas ocorrendo de forma simultânea;

5.11.4 Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;

5.11.5 Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente;

5.11.6 Se autenticar com o servidor utilizando um certificado de cliente, próprio da solução, com os mesmos atributos do certificado do cliente;

5.11.7 As listas de acesso devem ser baseadas nos atributos de um certificado.

5.12 Deve permitir ações caso o certificado original do servidor não seja confiável ou esteja expirado;

5.13 Deve permitir "by-pass" do tráfego caso o TLS handshake falhe;

5.14 Deve permitir a verificação da validade do certificado digital apresentado:

5.14.1 Pelo cliente através de Listas de Certificados Revogados (LCR) ou através de listas;

5.14.2 Via OCSP (Online Certificate Status Protocol);

5.15 Deve usar sempre o último arquivo LCR para a consulta de Lista de Certificados Revogados;

5.16 Deve implementar os protocolos TLS versões 1.1, 1.2 e 1.3;

5.17 Deve manter e gerenciar todo o tráfego criptografado com protocolo, TLS versões 1.1, 1.2 e 1.3;

5.18 Deve implementar o algoritmo de hash SHA1;

5.19 Deve implementar renegociação de sessão;

5.20 Deve possuir os seguintes algoritmos de encriptação: 3DES, RSA, AES128 e AES-256, ECCDHE (P-256 e P-384) e algoritmo de autenticação ECDSA;

5.21 Deve permitir geração de chaves RSA, enrollment de certificado, importação e exportação de chaves, certificados de servidores, e checagem de LCR (Lista de Certificados Revogados);

5.22 Por direcionamento inteligente de tráfego SSL entende-se a capacidade de abrir o tráfego SSL de entrada

("INBOUND") encaminhá-lo, de forma seletiva, levando em conta o contexto de serviço, às diferentes soluções de segurança que estão no ambiente de Data Center. No âmbito deste projeto serão exigidas, no mínimo, as integrações com as soluções de NG Firewall.

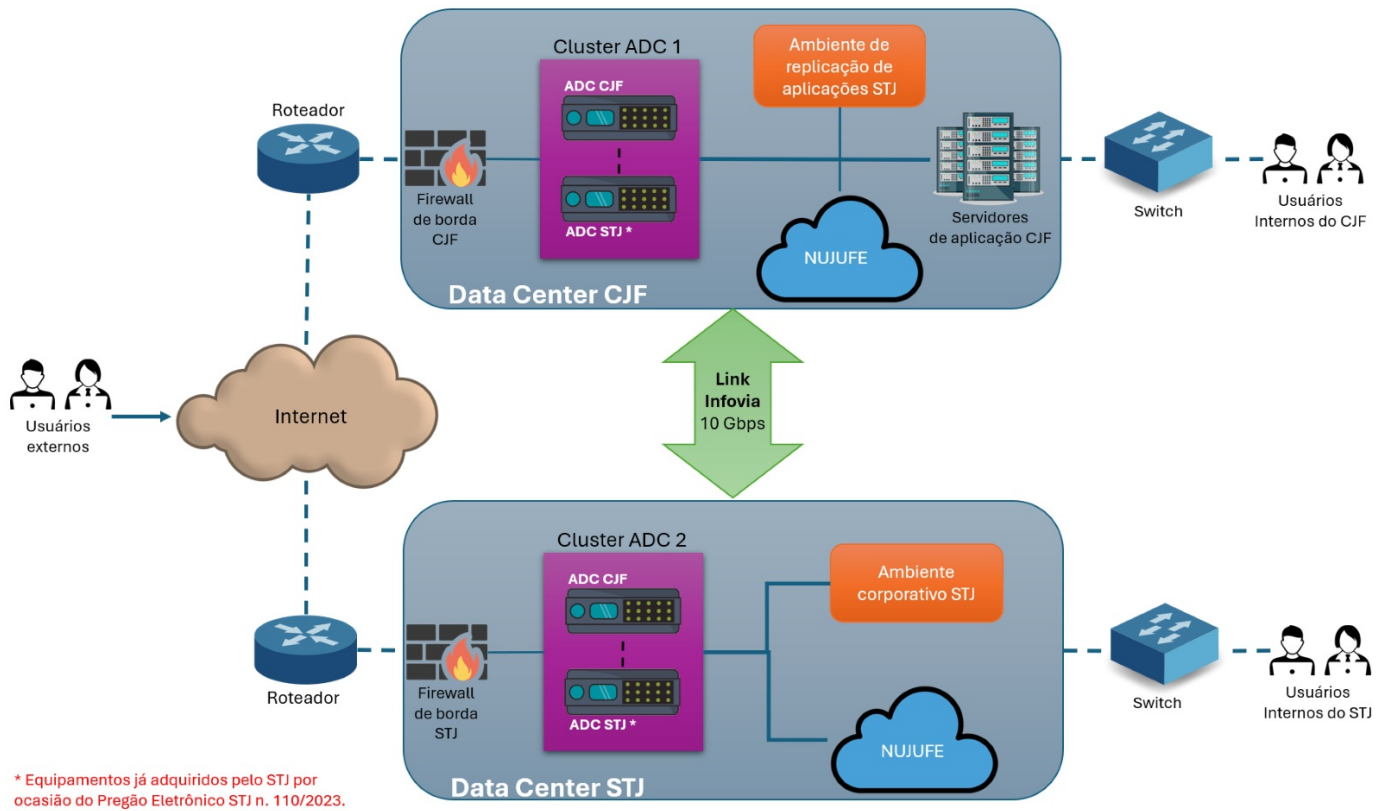
- 5.23 Deve suportar pelo menos as seguintes cifras e protocolos: TLS 1.1, 1.2 e 1.3, SHA, SHA2, AES-GCM, AES;
- 5.24 Deve implementar geração de chaves RSA, enrollment de certificado, importação e exportação de chaves, certificados de servidores.
- 5.25 Deve terminar as conexões SSL com a finalidade de inspecioná-las.
- 5.26 Deve proteger de ataques de negação de serviço que utilizem SSL.
- 5.27 Deve ser possível descobrir ameaças ocultas no SSL/TLS e prevenir ataques em vários estágios, usando as soluções de segurança já existentes assim como novas soluções que venham a ser adquiridas futuramente, independente de marca/modelo.
- 5.28 Deve ter capacidade de gerenciar o tráfego SSL do lado do cliente para o servidor, ou seja, deve ser capaz de decifrar todo o tráfego de entrada.
- 5.29 Deve suportar ECDHE, RSA e DHE com suporte a Forward Secrecy.
- 5.30 Deve suportar SSL Forward Secrecy como uma forma de melhorar a segurança nas transações SSL/TLS. Deve ser capaz de criar múltiplos Service Chains.
- 5.31 Deve suportar a renegociação de sessão;
- 5.32 Deve possibilitar a monitoração e gerenciamento independente de cada dispositivo da cadeia de inspeção. Deve possuir um mecanismo de classificação contextual do tráfego que será enviado para cada dispositivo.
- 5.33 Deve fazer a monitoração dos serviços dentro da camada de inspeção
- 5.34 Deve permitir a resiliência dos serviços dentro da zona de inspeção, inclusive fazendo o balanceamento de carga entre múltiplos equipamentos do mesmo serviço.
- 5.35 Deve permitir escalar os dispositivos de segurança com alta disponibilidade, usando testes de monitoração de saúde para identificar o estado de cada equipamento de segurança.
- 5.36 Deve ser possível prevenir ameaças de entrada (Data Center) e de saída (usuários), incluindo ataques de exploração, retorno de chamada e extração de dados.

6 DO GERENCIAMENTO LOCAL

- 6.1 Deve possuir funcionalidade de emissão de relatório gerencial/estatístico dos acessos em ferramenta local ou remota, além do syslog ou log interno, que contenham, no mínimo:
 - 6.1.1 Quantidade de acessos por VIP;
 - 6.1.2 Possuir MIB SNMP.
 - 6.1.3 Quantidade de acessos por serviços e servidores;
 - 6.1.4 Quantidade de usuários conectados;
 - 6.1.5 Disponibilidade dos serviços/VIP;
 - 6.1.6 Tempo de latência do cliente e servidor;
 - 6.1.7 Throughput de requisição e resposta;
 - 6.1.8 Transações por segundo;
 - 6.1.9 Quantidade de requisições por período;
 - 6.1.10 7.1.10. Quantidade de sessões;
 - 6.1.11 7.1.11. Retenção de logs para análise posterior;
- 6.2 Deve ser disponibilizada documentação das API dos appliances que compõem a solução;
- 6.3 Deve ser capaz de analisar a performance de aplicações web.
- 6.4 Deve gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, troubleshooting, planejamento de capacidade e análise da experiência dos usuários finais no acesso às aplicações.

- 6.5 Deve, a partir das informações coletadas, permitir a análise dos dados por aplicações, por URLs, por clientes e por servidores, permitindo, assim, a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução.
- 6.6 Deve gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados. Caso a solução não possua este recurso nativamente poderá ser aceito solução de terceiros para atendimento da especificação.
- 6.7 Deve permitir o detalhamento do tempo de resposta total de carregamento de uma URL/página.
- 6.8 Deve suportar mecanismos para criar usuários com no mínimo três conjuntos distintos de privilégios, sendo um deles somente leitura das configurações, para acesso às funções de gerenciamento dos equipamentos, via protocolos SSH, SNMP ou HTTPS.
- 6.9 Deve possibilitar a coleta de dados de gerenciamento dos equipamentos utilizando os protocolos SNMPv2c e SNMPv3.
- 6.10 Deve suportar MIB SNMP.
- Deve permitir a configuração de endereços IPs para o envio de traps SNMP (alarmes).

ANEXO III – ARQUITETURA PROPOSTA PARA INSTALAÇÃO DA SOLUÇÃO NO CJF



ANEXO IV – CRONOGRAMA DE IMPLANTAÇÃO

Prazo Máximo (em dias corridos)	Descrição do evento ou atividade a ser realizada	Responsável pela atividade
OSFB	Emissão da Ordem de Serviço e Fornecimento de Bens	CONTRATANTE
RIP = OSFB + 5	Reunião de Inicial de Planejamento (RIP) e apresentação do Preposto, Gerente de Projetos e Responsável Técnico por parte da CONTRATADA.	CONTRATANTE e CONTRATADA

PI = RIP + 10	Entrega do Plano de Implantação	CONTRATADA
E = OSF + 45	Entrega dos <i>softwares</i> e equipamentos da solução	CONTRATADA
TRP1 = E + 5	Emissão do primeiro Termo de Recebimento Provisório (TRP1) da etapa de entrega dos equipamentos e <i>softwares</i> da solução.	CONTRATANTE
INST = TRP1 + 20	Instalação e configuração dos equipamentos e <i>softwares</i> da solução e entrega das licenças de uso	CONTRATADA
TRP2 = INST + 5	Emissão o Termo de Recebimento Provisório (TRP2) da etapa de instalação e configuração dos <i>softwares</i> e equipamentos da solução e entrega das licenças de uso	CONTRATANTE
TRD = TRP2 + 10	Emissão o Termo de Recebimento Definitivo (TRD) da etapa da entrega, instalação, configuração e licenciamento da solução.	CONTRATANTE
TC = TRD + 20	Início do período para emissão de Ordem(ns) de Serviço específica(s) para a ação de Transferência de Conhecimento.	CONTRATANTE

ANEXO V – PLANILHA DE COMPOSIÇÃO DE CUSTOS (ID. 0701697)

Anexo VI – Termo de confidencialidade e sigilo da Contratada

1. A empresa [RAZÃO/DENOMINAÇÃO SOCIAL], pessoa jurídica com sede em [ENDEREÇO], inscrita no CNPJ/MF com o n.º [N.º DE INSCRIÇÃO NO CNPJ/MF], neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente EMPRESA RECEPTORA, por tomar conhecimento de informações sobre o ambiente computacional do Conselho da Justiça Federal – CJF, aceita as regras, condições e obrigações constantes do presente Termo.
2. O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do CJF reveladas à EMPRESA RECEPTORA em função da prestação dos serviços objeto do contrato n.º XX/XXX.
3. A expressão “informação restrita” abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outros.
4. A EMPRESA RECEPTORA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do CJF, das informações restritas reveladas.
5. A EMPRESA RECEPTORA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao CJF, as informações restritas reveladas.
6. A EMPRESA RECEPTORA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao CJF, devendo cientificá-los da

existência deste Termo e da natureza confidencial das informações restritas reveladas.

7. A EMPRESA RECEPTORA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

8. A EMPRESA RECEPTORA obriga-se a informar imediatamente ao CJF qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

9. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CJF, possibilitará a imediata rescisão de qualquer contrato firmado entre o CJF e a EMPRESA RECEPTORA sem qualquer ônus para o CJF. Nesse caso, a EMPRESA RECEPTORA, estará sujeita, por ação ou omissão, além das multas definidas no Termo de Referência, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CJF, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

10. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do CJF.

11. E, por aceitar todas as condições e as obrigações constantes do presente Termo, a EMPRESA RECEPTORA assina o presente termo através de seus representantes legais.

Brasília, _____ de _____ de 202____.

ASSINATURA DO REPRESENTANTE DA CONTRATADA

ANEXO VII – TERMO DE VISTORIA

Declaro que eu, _____, portador(a) do CPF(MF) nº _____, representante da empresa _____, estabelecida no endereço _____, como seu(sua) representante legal para os fins da presente declaração, tomei conhecimento, com o objetivo de participação no Pregão N._____, de todas as informações necessárias à execução dos serviços licitados e que vistoriei os locais de instalação dos equipamentos e componentes.

Brasília, _____ de _____ de 202____.

ASSINATURA DO RESPONSÁVEL TÉCNICO/ REPRESENTANTE

ASSINATURA DO REPRESENTANTE DO CJF

Processo nº0000919-34.2024.4.90.8000

SEI nº0735724



Documento assinado eletronicamente por **Geraldo Costa Cavalcante Neto, Chefe - Seção de Apoio ao Planejamento das Contratações**, em 10/07/2025, às 17:19, conforme art. 1º, §2º, III, b, da [Lei 11.419/2006](#).



Documento assinado eletronicamente por **Gabriel Oliveira Menezes, Chefe - Seção de Suporte à Infraestrutura**, em 10/07/2025, às 17:30, conforme art. 1º, §2º, III, b, da [Lei 11.419/2006](#).



Documento assinado eletronicamente por **Adriana Jesus de Moraes, Subsecretária de Tecnologia e Suporte Técnico, em exercício**, em 10/07/2025, às 17:42, conforme art. 1º, §2º, III, b, da [Lei 11.419/2006](#).



A autenticidade do documento pode ser conferida no site https://sei.cjf.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0735724** e o código CRC **455CE316**.