TRIBUNAL SUPERIOR ELEITORAL

ANEXO I DO EDITAL - TERMO DE REFERÊNCIA

EDITAL DE LICITAÇÃO TSE Nº 53/2023

MODALIDADE: PREGÃO

FORMA: ELETRÔNICA

1. OBJETO

1.1. Renovação de garantias e licenciamentos de solução de segurança da informação e balanceamento de carga (ADC) de propriedade do TSE (Grupo 1), bem como expansão tecnológica de solução de segurança da informação e balanceamento de carga (ADC) incluindo garantias e serviços agregados de instalação e suporte técnico especializado (Grupo 2), consoante especificações, exigências e prazos constantes deste Termo de Referência.

2. JUSTIFICATIVA

2.1. A fundamentação da presente contratação e de seus quantitativos, assim como a descrição da solução como um todo, encontram-se pormenorizadas no Estudo Técnico Preliminar, Documento SEI nº 2461365.

3. ESPECIFICAÇÃO E FORMA DE EXECUÇÃO DO OBJETO

3.1. DESCRIÇÃO DO OBJETO

Grupo	Item	Descrição	Unidade de Fornecimento	Quantidade
1 (Renovação)	1	Renovação de garantia e licenciamento por 36 meses para appliances (ADC) F5 BIG-IP i5800	Unidade	4
	2	Serviço de suporte técnico especializado (36 meses prorrogáveis)	Meses	36
	3	Renovação tecnológica – Instalação e configuração (por appliance - ADC) para Item 1	Unidade	4
2 (Expansão)	4	Componente hardware da expansão tecnológica - Appliance de alta capacidade (ADC) F5 BIG-IP r10600	Unidade	2
	5	Componente software de gerenciamento e licenciamento da expansão tecnológica (ADC) – licenciamento e subscrições por 60 meses	Unidade	2
	6	Garantia da expansão tecnológica – Garantia do fabricante para hardware e software (ADC) por 60 meses	Unidade	2
	7	Instalação da expansão tecnológica – Instalação e configuração (por appliance - ADC)	Unidade	2

3.1.1. A empresa deverá encaminhar proposta de preços especificando marca e modelo do produto ofertado, conforme modelo de proposta contido no Anexo I-II deste Termo de Referência, além de apresentar tabela de atendimento ponto a ponto das especificações exigidas neste Termo de Referência.

3.1.2. Para todos os grupos, será exigida a comprovação de qualificação técnica, conforme estabelecido no Edital da Licitação.

3.2. DETALHAMENTO DO OBJETO

3.2.1. **<u>GRUPO 1 - ITEM 1: Renovação de garantia e licenciamento por 36 meses para appliances (ADC) F5 BIG-IP i5800</u>**

3.2.1.1. A contratada deverá fornecer renovação de garantia de 36 meses para os todos os hardwares, softwares e licenças dos equipamentos F5 Big IP i5800 de propriedade do TSE.

3.2.1.2. Os números de série dos equipamentos para os quais deverão ser providas as garantias são:

a) f5-ikfr-pxvi
b) f5-jnsp-cuaq
c) f5-uwcg-lknp
d) f5-ngcw-rwac

3.2.1.3. A garantia deve ser provida pelo fabricante dos equipamentos, na modalidade Premium (regime de atendimento 24x7 com suporte ininterrupto, 24 horas por dia, 7 dias da semana, incluindo feriados), e deverá abranger todos os elementos da solução, garantindo sua substituição, atualização e correto funcionamento pelo período de 36 meses.

3.2.1.4. A garantia deverá permitir que o TSE acione o fabricante diretamente para abertura de chamados de suporte e manutenção dos equipamentos e sistemas que compõem a solução, durante a nova vigência da garantia.

3.2.1.5. A contratada deverá providenciar permissão de acesso ao sítio do fabricante para acompanhamento pelo TSE de chamados, download e acesso a documentações, patches, fixes, firmwares, arquivos de qualquer tipo e/ou qualquer outro material referente à solução.

3.2.1.6. Deverá ser provida manutenção corretiva, com fornecimento de peças originais do fabricante.

3.2.1.7. A manutenção corretiva englobará todos os procedimentos destinados a recolocar os equipamentos em seu perfeito estado de uso, compreendendo, inclusive, substituições de peças (desde que constem no catálogo do fabricante identificadas com um part number) e equipamentos e ajustes de software necessários, de acordo com os seus manuais e normas técnicas específicas.

3.2.1.8. A contratada, sem ônus adicional para o TSE, será responsável por quaisquer despesas relacionadas ao deslocamento do seu(s) técnico(s) ao local da instalação e do exercício da garantia do equipamento, seja para retirada e/ou entrega, incluindo todas as despesas de transporte, frete e seguro correspondentes.

3.2.1.9. As peças ou os equipamentos substitutos deverão ser entregues nas dependências do TSE em até 10 (dez) dias úteis a partir da necessidade identificada e formalizada no processo de manutenção.

3.2.2. <u>GRUPO 1 - ITEM 2: Serviço de suporte técnico especializado</u>

3.2.2.1. O serviço deverá ser provido por meio de disponibilização de recurso humano no total de 240 (duzentas e quarenta) horas anuais de serviço;

3.2.2.2. Os serviços serão demandados por meio de emissão de Ordem de Serviço (OS) pelo contratante;

3.2.2.3. As OS deverão ser demandadas ordinariamente com, pelo menos, 5 (cinco) dias úteis de antecedência.

3.2.2.4. Cada OS emitida terá um mínimo de 08 horas de serviço.

3.2.2.5. Caso as atividades possam ocasionar indisponibilidade dos serviços dos equipamentos, deverão ser realizadas fora do horário comercial, em período noturno ou finais de semana, a critério do TSE.

3.2.2.6. As atividades a serem realizadas envolverão:

3.2.2.6.1. atuar como fornecedor de informações gerais relacionadas aos equipamentos e softwares da F5, bem como em potenciais melhoras que podem ser feitas na configuração da solução;

3.2.2.6.2. auxiliar na aplicação de configurações, atualizações de versões e implementação de novos serviços, revisando as etapas envolvidas antes de serem colocadas em produção;

3.2.2.6.3. prover assistência operacional da solução (adicionando, modificando ou removendo configurações);

3.2.2.6.4. atualizar a documentação do projeto da solução, em até 5 (cinco) dias úteis, sempre que mudanças forem implementadas com sucesso;

3.2.2.6.5. realizar inspeção nos equipamentos para garantir que as configurações estejam consistentes com o projeto e atualizadas com todas as mudanças implementadas em até 5 (cinco) dias úteis da implementação;

3.2.2.6.6. participar da resolução de tickets de suporte em aberto, atuando de forma eficaz na coleta de informações relevantes para subsidiar os casos abertos e promovendo a melhoria dos tempos de solução;

3.2.2.6.7. auxiliar na revisão das configurações das políticas de segurança de modo a garantir que esteja consistente com as melhores práticas e recomendações do fabricante;

3.2.2.6.8. coordenar briefings e sessões avançadas com os especialistas de produto F5 sobre tópicos que são pertinentes ao ambiente e aos objetivos da organização e promover rodadas de discussões com seus pares

3.2.2.6.9. elaborar relatório mensal com as atividades executadas, o planejamento para o mês seguinte, recomendações técnicas e outras informações relevantes da solução.

3.2.2.6.10. Atualização de firmware;

3.2.2.6.11. Atualização de software de gerenciamento

3.2.2.6.12. Health-check para reduzir a probabilidade de falha ou a degradação do funcionamento da solução;

3.2.2.7. Os serviços terão duração de 36 meses, podendo ser prorrogados nos limites legais.

3.2.2.8. Os serviços cobrirão 06 (seis) appliances de equipamentos F5 BigIP.

3.2.2.9. Os Serviços deverão ser prestados por profissional(is) com amplo conhecimento da solução ofertada, com acesso e domínio de ferramentas, sistemas e aplicações do fabricante que apoiem as atividades descritas, devendo possuir no mínimo as seguintes certificações vigentes:

3.2.2.9.1. F5 Certified Administrator (F5-CA);

3.2.2.9.2. F5 Certified Technical Specialist (F5-CTS);

3.2.2.10. A comprovação das certificações do(s) profissional(ais) que realizará(ão) o suporte previstas no item **3.2.2.4.** deste Termo de Referência deverá ser realizada no momento da abertura da ordem de serviço.

3.2.2.10.1. Caso as execuções subsequentes do suporte sejam realizadas por profissional que já hajam apresentado essas credenciais, não haverá a necessidade de nova apresentação na abertura da ordem de serviço.

3.2.2.11. A lista de atribuições e serviços descrita no item **3.2.2.6.** não é exaustiva, cabendo ao Contratante adequar na ordem de serviço outras demandas pertinentes ao suporte técnico da solução de ADC.

3.2.3. <u>GRUPO 1 - ITEM 3: Renovação tecnológica – Instalação e configuração para Item 1</u>

3.2.3.1. PROJETO EXECUTIVO

3.2.3.1.1. Em até 30 dias corridos após a assinatura do contrato, a Contratada deverá submeter o documento contendo o Projeto Executivo para a aprovação do TSE.

3.2.3.1.2. O TSE poderá recusar, em parte ou totalmente o projeto executivo, desde que esse não atenda as especificações deste Anexo ou esteja incompleto. Nesse caso, será concedido prazo adicional de até 15 dias corridos à Contratada para realizar as devidas adequações.

3.2.3.1.3. O Projeto Executivo deve contemplar, minimamente:

a) a identificação e contatos de telefone e correio eletrônico do Gerente de Projeto;

b) o cronograma detalhado de implantação, contendo o impacto e o esforço das etapas;

c) a arquitetura dos equipamentos em relação ao cenário do TSE, contendo diagrama de rede com principais elementos;

d) a lista de acessórios a serem entregues, seus part numbers, seriais e licenças, caso estejam disponíveis para a contratada;

e) o quadro resumo das atividades e o responsável pela sua execução.

3.2.3.2. RELATÓRIOS QUINZENAIS

3.2.3.2.1. A partir da entrega do Projeto Executivo, deverão ser encaminhados relatórios quinzenais de recepção e providências até que a última pendência de entrega e instalação esteja resolvida.

3.2.3.2.2. Esses relatórios devem ser entregues via e-mail ao Fiscal do Contrato, que poderão contestá-los.

3.2.3.2.3. Esses relatórios deverão conter, minimamente, informações no seu intervalo de tempo sobre:

a) entregas realizadas;

b) decisões relevantes tomadas;

c) dúvidas existentes;

d) pendências e suas motivações.

3.2.3.3. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

3.2.3.3.1. Do Gerente de Projeto

3.2.3.3.1.1. A contratada deve alocar, às suas expensas, um Gerente de Projeto com experiência em implantação de projetos de Tecnologia da Informação (TI), com as seguintes atribuições mínimas:

a) garantir a execução de todos os aspectos do contrato assinado entre o TSE e a contratada;

b) garantir prazos e qualidade dos serviços;

c) elaborar e manter atualizado o cronograma de atividades e manter informado o Gestor de Contrato do TSE da evolução dos serviços sempre que for solicitado;

d) ser o ponto focal do TSE para todas as comunicações e solicitações referentes ao projeto junto à contratada, incluindo questões referentes a faturamento, pagamento, emissão e conferência de notas fiscais, conferência de volumes e especificações, envio de licenças e eventuais problemas com profissionais alocados pela contratada.

3.2.3.3.1.2. Ficará a cargo desse profissional a emissão de relatórios quinzenais.

3.2.3.3.1.3. Os custos referentes ao Gerente de Projeto e às equipes destinadas ao apoio e à execução do projeto (instalações dos equipamentos nas dependências do TSE, migrações e demais implementações necessárias) deverão estar contemplados na Proposta de Preços Ajustada, não cabendo nenhum custo adicional ao TSE.

3.2.3.3.1.4. A Contratada deverá repassar ao TSE todas as senhas do sistema. Ficará a critério daa equipe técnica do TSE alterá-las segundo sua conveniência.

3.2.3.4. REQUISITOS DE IMPLANTAÇÃO

3.2.3.4.1. As configurações e ajustes dos serviços nos equipamentos F5 em uso, deverão ser realizadas pela contratada em janelas definidas pelo TSE e deverão constar no projeto executivo.

3.2.3.4.1.1. Deverá constar no projeto a implantação e ativação do novo licenciamento fornecido por meio do Item 1 deste Termo de Referência, preservando-se todas as configurações existentes nos equipamentos, bem como assegurando a continuidade de funcionamento dos sistemas do TSE.

3.2.3.4.1.2. Nas configurações e ajustes do ambiente corporativo, a contratada deverá realizar o redimensionamento e ajustes de parâmetros, em consonância com o projeto aprovado pelo TSE, sem impacto nas funcionalidades.

3.2.4. GRUPO 2 - ITEM 4: Componente hardware da expansão tecnológica - Appliance de alta capacidade (ADC) F5 BIG-IP r10600

3.2.4.1. Consiste de fornecimento de appliances de alta capacidade modelo r10600 do fabricante F5.

3.2.4.2. O detalhamento das especificações técnicas a serem atendidas pelo appliance encontra-se no Anexo I-I deste Termo de Referência.

3.2.5. GRUPO 2 - ITEM 5: Componente software de gerenciamento e licenciamento da expansão tecnológica (ADC) – licenciamento e subscrições por 60 meses

3.2.5.1. Consiste de subscrição temporária de licenciamento de software de gerenciamento e licenciamento da expansão tecnológica (ADC) para appliance de alta capacidade modelo r10600 do fabricante F5.

3.2.5.2. A subscrição terá duração de 60 meses.

3.2.5.3. O detalhamento das especificações técnicas encontra-se no Anexo I-I deste Termo de Referência.

3.2.6. GRUPO 2 - ITEM 6: Garantia da expansão tecnológica – Garantia do fabricante para hardware e software (ADC) por 60 meses

3.2.6.1. A contratada deverá fornecer garantia durante 60 meses para os todos os hardwares, softwares e licenças dos equipamentos F5 r10600 de propriedade do TSE, contados da data de entrega dos equipamentos.

3.2.6.2. A garantia deve ser provida pelo fabricante dos equipamentos, na modalidade Premium (regime de atendimento 24x7 com suporte ininterrupto, 24 horas por dia, 7 dias da semana, incluindo feriados), e deverá abranger todos os elementos da solução, garantindo sua substituição, atualização e correto funcionamento pelo período de 60 (sessenta) meses, contados da data de entrega dos equipamentos.

3.2.6.3. A garantia deverá permitir que o TSE acione o fabricante diretamente para abertura de chamados de suporte e manutenção dos equipamentos e sistemas que compõem a solução, durante a vigência da garantia.

3.2.6.4. A contratada deverá providenciar permissão de acesso ao sítio do fabricante para acompanhamento pelo TSE de chamados, download e acesso a documentações, patches, fixes, firmwares, arquivos de qualquer tipo e/ou qualquer outro material referente à solução.

3.2.6.5. Deverá ser provida manutenção corretiva, com fornecimento de peças originais do fabricante.

3.2.6.6. A manutenção corretiva englobará todos os procedimentos destinados a recolocar os equipamentos em seu perfeito estado de uso, compreendendo, inclusive, substituições de peças (desde que constem no catálogo do fabricante identificadas com um part number) e equipamentos e ajustes de software necessários, de acordo com os seus manuais e normas técnicas específicas.

3.2.6.7. A contratada, sem ônus adicional para o TSE, será responsável por quaisquer despesas relacionadas ao deslocamento do seu(s) técnico(s) ao local da instalação e do exercício da garantia do equipamento, seja para retirada e/ou entrega, incluindo todas as despesas de transporte, frete e seguro correspondentes.

3.2.6.8. As peças ou os equipamentos substitutos deverão ser entregues nas dependências do TSE em até 10 (dez) dias úteis a partir da necessidade identificada e formalizada no processo de manutenção.

3.2.7. GRUPO 2 - ITEM 7: Instalação da expansão tecnológica – Instalação e configuração (por appliance - ADC)

3.2.7.1. PROJETO EXECUTIVO

3.2.7.1.1. Em até 30 dias corridos após a assinatura do contrato, a Contratada deverá submeter o documento contendo o Projeto Executivo para a aprovação do TSE.

3.2.7.1.2. O TSE poderá recusar, em parte ou totalmente o projeto executivo, desde que esse não atenda as especificações deste Anexo ou esteja incompleto. Nesse caso, será concedido prazo adicional de até 15 dias corridos à Contratada para realizar as devidas adequações.

3.2.7.1.3. O Projeto Executivo deve contemplar, minimamente:

3.2.7.1.3.1. a identificação e contatos de telefone e correio eletrônico do Gerente de Projeto;

3.2.7.1.3.2. o cronograma detalhado de implantação, contendo o impacto e o esforço das etapas;

3.2.7.1.3.3. a arquitetura dos equipamentos em relação ao cenário do TSE, contendo diagrama de rede com principais elementos;

3.2.7.1.3.4. a lista de equipamentos e acessórios a serem entregues, seus part numbers, seriais e licenças, caso estejam disponíveis para a contratada;

3.2.7.1.3.5. o quadro resumo das atividades e o responsável pela sua execução.

3.2.7.2. RELATÓRIOS QUINZENAIS

3.2.7.2.1. A partir da entrega do Projeto Executivo, deverão ser encaminhados relatórios quinzenais de recepção e providências até que a última pendência de entrega e instalação esteja resolvida.

3.2.7.2.2. Esses relatórios devem ser entregues via e-mail ao Fiscal do Contrato, que poderão contestá-los.

3.2.7.2.3. Esses relatórios deverão conter, minimamente, informações no seu intervalo de tempo sobre:

3.2.7.2.3.1. entregas realizadas;

3.2.7.2.3.2. decisões relevantes tomadas;

3.2.7.2.3.3. dúvidas existentes;

3.2.7.2.3.4. pendências e suas motivações.

3.2.7.3. AS BUILT

3.2.7.3.1. Deverá ser elaborado pela Contratada o as built das instalações efetuadas, contendo um descritivo detalhado das configurações lógicas e físicas da solução, não se restringindo, incluindo descritivo das configurações adotadas.

3.2.7.3.2. A entrega desse documento é uma das condições para a emissão do TRD.

3.2.7.4. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

3.2.7.4.1. Do Gerente de Projeto

3.2.7.4.1.1. A contratada deve alocar, às suas expensas, um Gerente de Projeto com experiência em implantação de projetos de Tecnologia da Informação (TI), com as seguintes atribuições mínimas:

a) garantir a execução de todos os aspectos do contrato assinado entre o TSE e a contratada;

b) garantir prazos e qualidade dos serviços;

c) elaborar e manter atualizado o cronograma de atividades e manter informado o Gestor de Contrato do TSE da evolução dos serviços sempre que for solicitado;

d) ser o ponto focal do TSE para todas as comunicações e solicitações referentes ao projeto junto à contratada, incluindo questões referentes a faturamento, pagamento, emissão e conferência de notas fiscais, conferência de volumes e especificações, envio de equipamentos e eventuais problemas com profissionais alocados pela contratada.

3.2.7.4.1.2. Ficará a cargo desse profissional a emissão de relatórios quinzenais.

3.2.7.4.1.3. Os custos referentes ao Gerente de Projeto e às equipes destinadas ao apoio e à execução do projeto (instalações dos equipamentos nas dependências do TSE, migrações e demais implementações necessárias) deverão estar contemplados na Proposta de Preços Ajustada, não cabendo nenhum custo adicional ao TSE.

3.2.7.4.1.4. A Contratada deverá repassar ao TSE todas as senhas do sistema. Ficará a critério do Banco alterá-las segundo sua conveniência.

3.2.7.5. REQUISITOS DE IMPLANTAÇÃO

3.2.7.5.1. As migrações dos serviços para os novos equipamentos F5, deverão ser realizadas pela contratada em janelas definidas pelo TSE e deverão constar no projeto executivo.

3.2.7.5.1.1. Nas migrações para os novos equipamentos no ambiente corporativo, a contratada deverá realizar o redimensionamento dos vcmp hospedados no hardware atual, em consonância com o projeto aprovado pelo TSE, sem impacto nas funcionalidades.

3.2.7.5.1.2. Deverá constar no projeto a migração das VE hospedadas em máquinas do TSE para os novos hardwares, o dimensionamento e as adequações necessárias na topologia e nas configurações para a implantação da nova solução, sem perda das funcionalidades em uso.

3.2.7.5.1.3. A contratada deverá integrar os novos equipamentos ao ambiente de rede do TSE, tendo como obrigação acessória o fornecimento de cabos DAC ou conjuntos de transceivers e fibras ópticas para interligação destes à rede de comunicação de dados do TSE. Os switches do TSE aceitam conexões de 10, 25 e 100GBPS.

3.3. PRAZO E LOCAL DE ENTREGA

3.3.1. Os produtos deverão ser entregues na Seção de Monitoramento da Produção - SEMOP, situada no Edifício Anexo do Tribunal Superior Eleitoral, Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2 Brasília/DF – 70095-901, no horário das 10h às 18h.

3.3.1.1. O prazo de entrega será de até 60 (sessenta) dias corridos, contados da data de início da vigência contratual.

3.3.1.2. A contratada deverá enviar com antecedência de 2 dias, mensagem eletrônica ao endereço semop.servidores@tse.jus.br para fins de agendamento da entrega.

3.3.2. Ao Tribunal Superior Eleitoral fica reservado o direito de recusar de pronto o produto que flagrantemente não esteja em conformidade com a descrição do item.

3.3.3. Os produtos deverão ser novos, não se admitindo, em hipótese alguma, o fornecimento de material/equipamento alternativo, reciclado, recondicionado ou recuperado.

3.3.4. Os produtos deverão ser entregues em embalagem original, sem avarias e respeitar toda legislação vigente referente ao objeto a ser fornecido.

3.3.5. A Contratada deverá estar apta à execução do suporte técnico nas dependências do Contratante, sito, ordinariamente no Edifício Anexo do Tribunal Superior Eleitoral, Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2 Brasília/DF – 70095-901 ou remotamente (em casos eventuais, conforme definido em ordem de serviço) em até 20 (vinte dias) contados da data de início da vigência contratual.

3.3.5.1. A execução dos serviços de suporte técnico deverá ser prestada ordinariamente no horário entre 7 horas e 21 horas em dias da semana, conforme definido em ordem de serviço ou emergencialmente (casos de interrupção completa da solução ou parcial que afetem serviços críticos do Contratante) a qualquer hora ou dia da semana, respeitados os limites de horas estabelecidos neste TR.

3.4. GARANTIA TÉCNICA

3.4.1. O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 36 meses para os itens do Grupo 1 e 60 (sessenta) meses para os itens do Grupo 2, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

3.4.2. A Contratada poderá subcontratar o fabricante dos equipamentos para a prestação de todos os serviços de garantia previstos neste Termo de Referência.

3.4.3. A garantia exigida dos itens da contratação será a garantia fornecida pelo fabricante ou provedor de serviços autorizado e credenciado pelo fabricante.

3.4.4. A garantia será prestada com vistas a manter os bens fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional ao Tribunal.

3.4.5. A garantia técnica deverá cobrir todo(s) o(s) equipamento(s), peças, softwares e componentes cotados neste Termo de Referência, com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional ao Tribunal.

3.4.6. A contratada deverá prestar, durante o período de garantia, assistência técnica contra defeitos de fabricação e suporte técnico referente ao uso de recursos dos equipamentos e à solução de problemas de funcionamento, durante a utilização normal dos equipamento e softwares, independente da existência de falha material.

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

3.4.6.2. Todas as peças e componentes mecânicos ou eletrônicos substituídos deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos utilizados na fabricação do(s) equipamento(s), sendo sempre novos e de primeiro uso.

3.4.6.3. A substituição de peças e/ou componentes mecânicos ou eletrônicos por outros de marcas e/ou modelos diferentes dos originais cotados pela contratada somente poderá ser efetuada em caso de descontinuidade do componente originalmente cotado na proposta e ainda mediante análise e autorização do TSE.

3.4.6.4. O prazo para substituição dos componentes que apresentarem vício ou defeito durante o prazo de garantia é de até o próximo dia útil, caso o equipamento esteja inoperante, e de até 5 (cinco) dias úteis, para os demais casos, ambos contados do recebimento da notificação do TSE.

3.4.6.5. O custo e a responsabilidade pelo recolhimento e entrega dos bens durante o prazo de garantia serão da Contratada.

3.4.6.6. Durante o período de garantia, Serviços de Suporte técnico poderão ser demandados em situações de contingência, em rotinas operacionais, no esclarecimento de dúvidas ou em períodos de mudanças complexas no ambiente que ensejem a incorporação temporária de expertise, para realizar tarefas de configuração ou ajuste da solução.

3.4.7. O atendimento deverá ser realizado na modalidade "24x7", ou seja, 24 horas por dia, sete dias por semana, incluindo-se feriados.

3.4.8. Deverá ser disponibilizada uma Central de Atendimento em português para abertura de chamado de Assistência Técnica disponível na modalidade "24x7".

3.4.9. A contratada poderá informar, adicionalmente, endereço de e-mail e/ou página na Internet para abertura de chamado.

3.4.10. A contratada poderá, adicionalmente, solicitar que os chamados sejam registrados diretamente com o fabricante dos produtos, bem como seus respectivos atendimentos.

3.4.11. O atendimento de hardware será do tipo “on site” mediante manutenção corretiva no local de instalação dos equipamentos e deverá cobrir todo e qualquer defeito apresentado, incluindo a substituição de peças, componentes, ajustes, reparos e correções necessárias.

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

3.5. NÍVEIS MÍNIMOS DE SERVIÇO

3.5.1. Os níveis de serviço a serem cumpridos para atendimento da assistência técnica são:

3.5.1.1. **Severidade 1** - problemas que tornem a solução inoperante. Uma solicitação de serviço severidade 1 tem uma ou mais das seguintes características:

a) dados corrompidos;

b) uma função crítica documentada não está disponível;

c) o sistema trava indefinidamente, causando demoras inaceitáveis ou indefinidas para recursos ou respostas;

d) o sistema falha repetidamente após tentativas de reinicializações.

3.5.1.2. **Severidade 2** - problemas ou dúvidas que prejudiquem a operação do equipamento, mas que não interrompem o acesso aos dados.

3.5.1.3. **Severidade 3** - problemas ou dúvidas que criam algumas restrições à operação do equipamento.

3.5.2. O prazo de início do atendimento e solução dos chamados técnicos deverá ocorrer conforme os níveis mínimo de serviço detalhados abaixo, contados da abertura de chamado:

Severidade	Disponibilidade para atendimento	Tempo máximo de atendimento *	Tempo de solução **	Glosa por descumprimento
1	24 horas por dia, 7 dias por semana	Deverão ser iniciados no prazo de **4 (quatro) horas**;	Deve ocorrer em até **6 horas** para solução de chamados de hardware e até **8 horas** para solução de contorno de problemas de software	0,5% do valor do Suporte Técnico dos serviços por hora que exceda o prazo de recuperação, de até 8 horas; 1% nas horas seguintes.
2	24 horas por dia, 7 dias por semana	Deverão ser iniciados no prazo de **8 (oito) horas úteis**;	Deve ocorrer em até **12 horas** para solução de chamados de hardware e até **24 horas** para solução de contorno de problemas de software	0,3% do valor do Suporte Técnico dos serviços por dia que exceda o prazo de recuperação; 0,5% nas horas seguintes.
3	24 horas por dia, 7 dias por semana	Deverão ser iniciados no prazo de **24 (vinte e quatro) horas úteis**;	Deve ocorrer em até o **próximo dia útil** para solução de chamados de hardware e até **7 dias corridos** para solução de contorno de problemas de software	0,1% do valor do Suporte Técnico dos serviços por dia que exceda o prazo de recuperação; 0,3% nas horas seguintes.

* Tempo de atendimento: Considera-se tempo de atendimento o tempo entre o registro do chamado até o primeiro contato realizado por técnico especialista do produto (nesse momento ainda não há solução para o problema).

** Tempo de solução: Considera-se tempo de solução o tempo gasto entre o registro do chamado até o momento onde é aplicada uma solução para restabelecer o serviço, eliminar prejuízos ou restrições de operação da solução ou que tenha a dúvida sanada.

3.6. INSTALAÇÃO

3.6.1. Todos os serviços de instalação e atualizações de versões previstos neste Termo de Referência deverão ser realizados no TSE e seguir as seguintes exigências obrigatórias para cada instalação:

3.6.1.1. As janelas de parada para instalação e configuração de cada hardware e software deste Termo de Referência deverão ser preferencialmente em horário comercial;

3.6.1.2. As instalações deverão ser realizadas sem que o serviço de ADC seja interrompido;

3.6.1.3. O serviço de instalação compreende as seguintes atividades:

3.6.1.4. O serviço de arquitetura e instalação deverá ser realizado por profissional devidamente certificado pelo fabricante do equipamento;

3.6.1.5. Previamente ou no ato da instalação deverá ser apresentada cópia da certificação válida do profissional que realizará a atividade;

3.6.1.6. A CONTRATADA deverá fornecer previamente um cronograma com o planejamento e levantamento de requisitos para cada serviço de instalação;

3.6.1.7. Deverá possuir todos os cabos e acessórios necessários à instalação do equipamento;

3.6.1.8. A CONTRATADA deverá realizar configurações e testes de funcionalidade do equipamento, inclusive com relação a realização de conectividade do ADC com um conjunto de aplicações definidas pelo TSE;

3.6.1.8.1. A CONTRATADA deverá analisar os elementos da infraestrutura do TSE envolvidos na arquitetura do ADC e verificar possíveis pontos de limitação que possam impedir o melhor desempenho da solução adquirida, podendo, a critério do TSE, realizar ajustes nas configurações desses elementos do TSE de forma a se obter o melhor desempenho do ADC.

3.6.1.9. O serviço de instalação física e lógica de cada hardware deste Termo de Referência, a energização e configuração e testes de funcionalidades serão realizadas nas instalações do TSE, em Brasília - DF.

3.6.1.10.1. Deverá ser emitido um relatório técnico ao final da instalação, contendo: Descritivo das atividades realizadas, part numbers e número de série do(s) equipamento(s) instalado(s) e cópia da certificação do profissional;

3.6.1.10. O relatório deve ser datado e assinado pelo técnico que realizou a atividade de instalação.

3.6.2. A instalação deverá ser concluída em até 10 (dez) dias úteis, contados do primeiro dia útil subsequente ao da entrega dos equipamentos.

3.6.3. O prazo acima poderá ser suspenso, a critério do TSE, durante a fase de testes de desempenho dos equipamentos.

3.7. VISTORIA TÉCNICA

3.7.1. Em virtude das peculiaridades de instalação e configuração nos ambientes seguros (Sala Cofre) do TSE, os representantes das licitantes poderão comparecer à Seção de Monitoramento e Produção - SEMOP localizada no edifício Anexo do TSE – sala AA15, no Setor de Administração Federal Sul (SAFS), Quadra 07, Lotes 1/2, Brasília – DF, CEP: 70095-901, para conhecer o ambiente, a infraestrutura, as condições e os locais onde serão instalados e configurados os hardwares que compõem o objeto deste Termo de Referência;

3.7.2. A contratada deverá integrar os novos equipamentos ao ambiente de rede do TSE. Para tanto recomenda-se a realização de vistoria para que haja medição de cabeamento necessário. Os switches do TSE aceitam conexões de 10, 25 e 100GBPS, no entanto há de ser fornecido cabos DAC ou conjuntos de transceivers e fibras ópticas para interligação destes à rede de comunicação de dados do TSE. A voltagem do datacenter do TSE é de 220V.

3.7.3. A vistoria técnica deverá ocorrer no horário marcado e ser agendada junto à equipe técnica do TSE pela conta de e-mail coinf@tse.jus.br;

3.7.4. As visitas deverão ser agendadas para o período compreendido entre 09 e 19h e deverá ser realizada até 24 (vinte e quatro) horas antes da data de abertura das propostas, por profissional designado pela licitante e por autorização da empresa;

3.7.5. A autorização ou procuração deverá ser emitida em papel timbrado e nela deverá constar informações sobre a identificação do profissional e da empresa, como nomes, CPF e CNPJ:

3.7.5.1. Esta autorização ou procuração deverá ser acompanhadas de cópia do Registro Geral do profissional indicado, e caso não seja apresentado o documento, serão fornecidos apenas informações e procedimentos que não promovam furos de segurança.

3.7.6. Antes de iniciar a vistoria técnica, o profissional designado deverá assinar **Termo de Confidencialidade,** constante do Anexo I-VI deste Termo de Referência, quanto às informações repassadas.

3.7.7. Após a vistoria técnica, o profissional deverá assinar o Termo de Vistoria, conforme modelo contido no Anexo I-V deste Termo de Referência, reconhecendo que fez a visita e teve ciência dos locais e condições de instalação e configuração, tipos de manutenção e suporte, modelos de equipamentos e sistemas operacionais; e dos procedimentos e regras para acesso às dependências do TSE.

3.7.8. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

3.7.9. Não será permitida vistoria de duas ou mais empresas concomitantemente.

3.8. FORMAS DE COMUNICAÇÃO E ACOMPANHAMENTO DA EXECUÇÃO DO CONTRATO

3.8.1. A comunicação entre o TSE e a Contratada durante a execução do contrato, far-se-á, preferencialmente, por meio do preposto designado pela contratada.

3.8.2. Poderão ser utilizados para a comunicação:

3.8.2.1. Ofícios;

3.8.2.2. Ordens de Serviço;

3.8.2.3. Mensagens escritas;

3.8.2.4. Relatórios de Medição e Relatórios em geral;

3.8.2.5. Termos de Recebimento;

3.8.2.6. Cartas; e

3.8.2.7. Demais documentos previstos em contrato ou neste Termo de Referência.

3.8.3. Sem prejuízo da necessidade de realização de reuniões periódicas, as comunicações devem se dar, preferencialmente, da seguinte maneira:

3.8.3.1. Questões administrativas durante a execução do contrato, que exijam comunicação formal:

1. Meio de Comunicação: correspondência física ou eletrônica, com aviso e/ou confirmação de recebimento, pessoalmente, por correio, ou por sistema informatizado de correio eletrônico;
2. Periodicidade: eventual ou conforme prazos previstos em contrato ou neste Termo de Referência.

3.8.3.2. Questões técnicas e/ou administrativas cotidianas, durante a execução do contrato:

1. Meio de Comunicação: correspondência eletrônica, telefone, sistemas ou qualquer outro forma acordada entre as partes, definidas na reunião inaugural;
2. Periodicidade: sempre disponível, em dias úteis, entre 9h e 19h.

3.8.3.3. Garantia Técnica:

1. Meio de Comunicação: página web, sistema informatizado, correspondência eletrônica, telefone;
2. Periodicidade: tempo integral (24 horas por dia, 7 (sete) dias por semana, 365 dias no ano)

4. RECEBIMENTO E PAGAMENTO

4.1. RECEBIMENTO

4.1.1. No momento da entrega, conforme as diretrizes contidas no item 3.2 desse Termo de Referência, os bens serão recebidos provisoriamente, de forma sumária, para posterior verificação de sua conformidade com as exigências contratuais.

4.1.1.1. Os itens a serem entregues deverão atender rigorosamente a todas as especificações técnicas exigidas e as apresentadas na proposta da contratada, inclusive no tocante às marcas, modelos de peças e/ou componentes internos, externos e consumíveis;

4.1.1.2. A contratada deverá entregar à Fiscalização Técnica todos os documentos necessários ao recebimento dos materiais previstos neste Termo de Referência.

4.1.2. O fiscal técnico ou comissão designada terão o prazo de 5 (cinco) dias úteis, contados do recebimento provisório, para emitir o Termo de Recebimento Definitivo - TRD e remeter o processo à fiscalização administrativa. O TRD compreenderá a verificação da conformidade do objeto aos termos contratuais, por meio das análises e conclusões dos quesitos previstos na Lista de Verificação contida no Anexo I-III deste Termo de Referência.

4.1.2.1. Identificada qualquer irregularidade pela fiscalização durante o recebimento do objeto, a Contratada deverá substituir os bens reprovados e cumprir as obrigações pendentes no prazo de 5 (cinco) dias úteis, contados da notificação.

4.1.2.2. Decorrido o prazo ou sanada a incorreção apontada pela fiscalização será reiniciado o prazo para emissão do TRD, nos termos do item 4.1.2.

4.1.2.3. O TSE poderá rescindir a contratação caso o objeto entregue seja novamente reprovado.

4.1.2.4. A contratada deverá recolher os bens reprovados no prazo de até 10 (dez) dias úteis. Caso não os recolha, poderão ser descartados ou doados.

4.1.2.5. O fiscal técnico ou a comissão designada, no caso de controvérsia sobre a execução do objeto quanto à dimensão, qualidade e/ou quantidade, deverá indicar, no TRD, a parcela incontroversa, a qual deve ser liberada para pagamento, nos termos do art. 143 da Lei nº 14.133/2021, sem prejuízo da aplicação das penalidades previstas no instrumento contratual.

4.1.3. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante, em conformidade com o art. 120 da Lei nº 14.133/21.

4.1.4. O recebimento dos serviços prestados, pertinentes a cada mês de execução contratual, será realizado por meio dos Termos de Recebimento Provisório - TRP e Definitivo - TRD - Anexo I - III deste Termo de Referência, emitidos pelo fiscal técnico ou comissão designada, até o 5º (quinto) dia útil do mês subsequente à prestação dos serviços.

4.1.5. O TRP será emitido com fundamento no que foi descrito na ordem de serviço, quando verificado o cumprimento das exigências de caráter técnico.

4.1.6. O TRD compreenderá a verificação da conformidade do objeto aos termos contratuais, com fundamento no trabalho feito pelo gestor ou pelo fiscal técnico e na verificação dos outros aspectos do contrato que não a execução do objeto propriamente dito, por meio das análises e conclusões dos quesitos previstos na Lista de Verificação/critérios de conferência contida no Anexo I – III.

4.1.7. A Contratada deverá reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, os serviços em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, além de cumprir quaisquer obrigações pendentes apontadas pela Fiscalização Técnica, em até 5 (cinco) dias úteis, contados da notificação.

4.1.7.1. Decorrido o prazo ou sanada a incorreção apontada pela fiscalização será reiniciado o prazo para emissão do TRD, nos termos do item 4.1.7.

4.1.8. O TRD contemplará também:

a) todas as evidências de descumprimento das obrigações assumidas pela Contratada, no todo ou em parte.

a.1) no caso de controvérsia sobre a execução do objeto quanto à dimensão, qualidade e/ou quantidade, deverá estar indicada no TRD a parcela incontroversa, a qual deve ser liberada para pagamento, nos termos do art. 143 da Lei nº 14.133/2021, sem prejuízo da aplicação das penalidades previstas neste Termo de Referência.

b) emissão de termo circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base em relatórios e documentação apresentados; e

c) comunicação à empresa para que emita a nota fiscal ou fatura com o valor exato dimensionado pela fiscalização.

4.1.9. A Contratada deverá entregar o faturamento com toda documentação exigida em contrato para liquidação e pagamento em até 5 (cinco) dias úteis, contados da emissão do TRD.

4.1.10. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade à fiscalização ou o acompanhamento pelo contratante, em conformidade com o art. 120 da Lei nº 14.133/21.

4.1.11. O recebimento provisório ou definitivo não excluirá do contratado a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

4.2. PAGAMENTO

4.2.1. O pagamento será efetuado até o 10º (décimo) dia útil, após o atesto da nota fiscal/fatura pelo servidor responsável, com a emissão de ordem bancária para o crédito em conta corrente da contratada, observada a ordem cronológica estabelecida no art. 141 da Lei nº 14.133/21.

4.2.1.1. O atesto do objeto contratado será feito pelo fiscal administrativo, designado pela autoridade competente, por meio da emissão de Nota Técnica de Atesto (NTA). O fiscal administrativo terá o prazo de 2 (dois) dias úteis para emitir a NTA e remeter o processo à unidade técnica responsável pelo pagamento, a partir do recebimento do documento fiscal, acompanhado do Termo de Recebimento Definitivo - TRD e dos demais documentos exigidos para liquidação e pagamento da despesa.

4.2.1.2. A Contratada deverá entregar o faturamento com toda documentação exigida para liquidação e pagamento em até 5 (cinco) dias úteis, contados da emissão do TRD.

4.2.1.3. A emissão de notas fiscais pelas empresas deve observar o regramento tributário, considerando que:

4.2.1.3.1. Os serviços pertinentes ao item 3 do Grupo 1 e itens 6 e 7 do Grupo 2 não se configuram obrigações acessórias à operação de venda do bem a ser adquirido. Extrapolam a garantia inerente ao equipamento e exigem parametrização customizada para o TSE, análise do ambiente de infraestrutura, replicação de configurações existentes. **Não devem** portanto, ser faturados juntamente com o bem por meio de nota fiscal de mercadorias. (vide Lei Complementar nº 87/1996, Lei 8.078/1990, dentre outras)

4.2.1.4. O pagamento a ser efetuado em favor da **CONTRATADA** estará sujeito à retenção na fonte de tributos e contribuições sociais de acordo com os normativos legais.

4.2.1.5. Na fase de liquidação e pagamento da despesa, a unidade de execução orçamentária e financeira realizará consulta *on-line* ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou nos sítios de cada órgão regulador, com fins de verificar a regularidade da contratada perante a Seguridade Social e a Fazenda Federal, o Fundo de Garantia por Tempo de Serviço e a Justiça Trabalhista.

4.2.2. O pagamento do item 2 do Grupo 01 deste Termo de Referência será efetuado mensalmente até o 10º (décimo) dia útil, após o atesto da nota fiscal/fatura pelo servidor responsável, com a emissão de ordem bancária para o crédito em conta corrente da contratada, observada a ordem cronológica estabelecida no art. 141 da Lei nº 14.133/21.

4.2.2.1. Aplicam-se ao item 4.2.2. as mesmas previsões estabelecidas nos itens de 4.2.1.1 a 4.2.1.5 deste Termo de Referência.

4.2.2.2. No primeiro e no último mês de vigência contratual, os valores serão rateados à base de 1/30 (um trinta avos), por dia, do valor mensal dos serviços, considerando-se o mês de 30 (trinta) dias. Nos meses subsequentes, os encargos da efetiva prestação dos serviços serão cobrados considerando-se o mês de 30 (trinta) dias.

5. OBRIGAÇÕES

5.1. OBRIGAÇÕES DA CONTRATADA

5.1.1. Executar, com observação dos prazos e exigências, todas as obrigações constantes deste Termo de Referência.

5.1.2. Responsabilizar-se pelas despesas decorrentes da execução do objeto deste Termo de Referência.

5.1.3. Informar, antes formalização da contratação, o nome do responsável (preposto), os contatos de telefone, e-mail ou outro meio hábil para comunicação com o TSE, bem como manter os dados atualizados durante toda a execução contratual, observado o disposto no item 3.8. deste Termo de Referência.

5.1.4. Acatar as recomendações efetuadas pelo fiscal do contrato.

5.1.5. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de culpa ou dolo na execução do objeto do Termo de Referência.

5.1.6. Fazer com que seus empregados se submetam aos regulamentos de segurança e disciplina durante o período de permanência nas dependências do TSE, não sendo permitido o acesso dos funcionários que estejam utilizando trajes sumários (shorts, chinelos de dedo, camisetas regatas ou sem camisa).

5.1.7. Comunicar ao TSE, imediatamente, por escrito, quando verificar condições inadequadas de execução do objeto ou a iminência de fatos que possam prejudicar a sua execução e prestar os esclarecimentos que forem solicitados pelos fiscais.

5.1.8. Manter o caráter confidencial dos dados e informações obtidos por qualquer meio ou prestados pelo TSE, não os divulgando, copiando, fornecendo ou mencionando a terceiros e nem a quaisquer pessoas ligadas direta ou indiretamente à contratada, durante e após a vigência do contrato, observados ainda, no que couber, as diretrizes vigentes adstritas à LGPD (Lei Geral de Proteção de Dados).

5.1.9. Manter, durante a execução do contrato, as condições de habilitação exigidas para a contratação.

5.1.9.1. Verificadas irregularidades nas condições que ensejaram sua habilitação quanto à regularidade fiscal, a contratada terá o prazo de 30 (trinta) dias corridos, contados da notificação da fiscalização, para regularizar a situação, sob pena de aplicação das penalidades cabíveis, sem prejuízo da rescisão do contrato a critério da Administração.

5.1.10. Responsabilizar-se pelos encargos trabalhistas, fiscais e comerciais resultantes desta contratação.

5.1.10.1. A inadimplência da contratada com referência aos encargos trabalhistas, fiscais e comerciais não transfere a responsabilidade por seu pagamento ao contratante, nem poderá onerar o objeto do contrato.

5.1.10.2. No caso de fornecimento de bens importados, a contratada deve apresentar a documentação que comprove a sua origem, bem como a quitação dos tributos de importação a eles referentes.

5.1.11. Fornecer máscaras N95 aos seus funcionários, em quantidade suficiente, para ingresso e permanência nas dependências do TSE, **quando houver a exigência** do uso por parte do Tribunal.

5.1.12. Orientar seus funcionários acerca da necessidade de observar protocolos sanitários definido pelo Contratante.

5.1.13. Não transferir a outrem, no todo ou em parte, o objeto deste Termo de Referência, salvo em caso de subcontratação autorizada.

5.1.13.1. A subcontratação autorizada é a prevista no item 3.4.2, que engloba o serviço de garantia técnica.

5.2. OBRIGAÇÕES DO CONTRATANTE

5.2.1. Prestar as informações e os esclarecimentos que venham a ser solicitados pela contratada.

5.2.2. Designar servidor ou comissão de servidores para fiscalizar a execução do objeto contratual.

5.2.3. Acompanhar, fiscalizar e atestar a execução contratual, bem como indicar as ocorrências verificadas, nos termos de normativo do TSE que disponha sobre os processos de contratação no âmbito do Tribunal.

5.2.4. Permitir que os funcionários da contratada, desde que devidamente identificados, tenham acesso aos locais de execução do objeto.

5.2.5. Recusar qualquer produto/serviço entregue em desacordo com as especificações constantes desse Termo de Referência ou com defeito.

5.2.6. Efetuar o pagamento à contratada, segundo as condições estabelecidas nesse Termo de Referência.

5.2.7. Realizar reunião inaugural antes do início efetivo da prestação dos serviços entre a fiscalização e a contratada.

6. DISPOSIÇÕES GERAIS

6.1. PRAZO DE VIGÊNCIA DO CONTRATO

6.1.1. O contrato terá vigência a partir de _____/_____/_____ e duração de:

a) 36 (trinta e seis) meses para o Grupo 1;

b) 05 (cinco) meses para o Grupo 2.

6.1.2. Os serviços de suporte técnico previstos no Item 2 do Grupo 1 poderão ser prorrogados nos termos da Lei. O mesmo não ocorrerá para os demais itens do Grupo 1.

6.2. CRITÉRIOS DE SUSTENTABILIDADE

6.2.1. Comprovar, como condição para participação na licitação, não possuir inscrição no cadastro de empregadores que tenham submetido trabalhadores a condições análogas à de escravo (Portaria Interministerial MTPS/MM/IRDH nº 4/2016).

6.2.1.1. A comprovação desse critério será efetuada a partir da consulta ao Cadastro acima mencionado, no sítio eletrônico (https://www.gov.br/trabalho-e-emprego/pt-br/assuntos/inspecao-do-trabalho/areas-de-atuacao/cadastro_de_empregadores.pdf), no qual consta lista emitida pelo Ministério do Trabalho e Emprego.

6.2.2. Comprovar, como condição para contratação, não ter sido condenada, a empresa e seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta ao previsto nos arts. 1º e 170 da Constituição Federal de 1988; no art. 149 do Código Penal; no Decreto nº 5.017/2004 (promulga o Protocolo de Palermo) e nas Convenções nºs 29 e 105 da Organização Internacional do Trabalho.

6.2.2.1. Deverá ser apresentada Certidão Judicial de Distribuição ("nada consta" ou "certidão negativa") **da esfera criminal, da Justiça Comum, Federal e Estadual,** da empresa e de seus dirigentes.

6.2.3. Consoante os normativos vigentes e pertinentes à sustentabilidade, a(s) Contratada(s) deverá(ão):

6.2.3.1. Apresentar, conjuntamente com a proposta de fornecimento, o(s) comprovante(s) de registro no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais (CTF/APP) do Ibama, relacionados às categorias e atividades listadas abaixo, acompanhado(s) do(s) respectivo(s) Certificado(s) de Regularidade (CR) válido(s): Categoria 05 - Indústria de Material Elétrico, Eletrônico e Comunicações; Atividade 5-2 - Fabricação de material elétrico, eletrônico e equipamentos para telecomunicação e informáticas.

6.2.3.1.1. Caso a proponente não seja fabricante do produto, mas, sim, revendedora, distribuidora ou lojista em geral e, por conseguinte, não desempenhe diretamente atividades poluidoras ou utilizadoras de recursos ambientais, fugindo, portanto, da obrigação de registro diante da instituição responsável, deverá apresentar o registro e a certificação do fabricante fornecedor do produto.

6.2.3.1.2. Para todos os casos em que a atividade estiver desobrigada de inscrição no CTF/APP do Ibama, a proponente deverá apresentar declaração assinada pelo responsável legal, constando a Lei nº 6.938/81 e a IN Ibama nº 13/2021, que desobrigam a inscrição da atividade constante do seu código CNAE - Classificação Nacional de Atividades Econômicas.

6.2.3.1.3. Nos casos em que o produto for importado e não havendo norma ambiental ou acordo setorial que preveja ao comerciante a obrigatoriedade do CTF de bem importado, a proponente deverá apresentar declaração correspondente de que o produto é importado, com a apresentação de documento comprobatório, sendo dispensada a apresentação do documento exigido no item 6.2.3.1 deste Termo de Referência.

6.2.4. A(s) Contratada(s) deverá(ão) ainda:

a) Comprovar a eficiência energética do equipamento mediante apresentação de certificado emitido por instituições públicas ou privadas;

b) Atender a diretiva RoHS (Restriction of Hazardous Substances) quanto a não utilização de substâncias nocivas ao Meio Ambiente;

c) Garantir que todos os resíduos sólidos gerados pelos produtos fornecidos que necessitam de destinação ambientalmente adequada (incluindo embalagens vazias) deverão ter seu descarte adequado, obedecendo aos procedimentos de logística reversa, em atendimento à Lei nº 12.305/2010 - Política Nacional de Resíduos Sólidos; e

d) Os equipamentos devem estar em conformidade com a norma IEC 60950 para segurança do usuário contra incidentes elétricos e combustão dos materiais elétricos.

6.2.5. Caso possuam 100 (cem) ou mais empregados, atender ao disposto no art. 93 da Lei nº 8.213/91, que determina a obrigatoriedade do preenchimento de 2 a 5% dos seus cargos com beneficiários reabilitados ou com pessoas com deficiência habilitadas, na seguinte proporção:

I - até 200 empregados: 2%;

II - de 201 a 500: 3%;

III - de 501 a 1.000: 4%; e

IV - de 1.001 em diante: 5%.

6.2.5.1. A comprovação será feita mediante declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, nos termos do Inciso IV do Art. 63 da Lei 14.133/2021.

6.2.6. Adota-se na especificação, como medida sustentável, a obrigação da contratada de entregar, em meio digital, todos os documentos produzidos ao longo do contrato.

ANEXO I-I - ESPECIFICAÇÕES TÉCNICAS

1. Requisitos gerais do componente hardware da expansão tecnológica - Appliance de alta capacidade (ADC) F5 r10600

1.1. Os equipamentos desta solução devem ser equipamentos físicos de mesmo fabricante, modelo, versão e licenciamento, sendo essa exigência requisito técnico fundamental para configuração de dispositivos que operarão em modo cluster;

1.2. O hardware e software que executarão os recursos e funcionalidades dessa camada de proteção deverão ser do tipo appliance físico, com hardware e software desenvolvidos para essa finalidade;

1.3. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.5. Possuir fontes de alimentação redundantes AC bivolt internas, com ajuste automático de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz), capaz de sustentar a carga de todo o equipamento com todas as portas ativas com apenas umas das fontes instalada e permitir a troca da fonte redundante com o equipamento em pleno funcionamento;

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

1.7. Possuir, no mínimo, as características de desempenho e conectividade:

1.7.1. Suportar, no mínimo, 190 (cento e noventa) Gbps em camada 4 do modelo OSI;

1.7.2. Suportar, no mínimo, 125 (cento e vinte e cinco) Gbps em camada 7 do modelo OSI;

1.7.3. Suportar, no mínimo, 1,9 (um vírgula nove) milhões de conexões por segundo na camada 4 do modelo OSI;

1.7.4. Suportar, no mínimo, 145 (cento e quarenta e cinco) milhões de conexões simultâneas na camada 4 do modelo OSI;

1.7.5. Suportar, no mínimo, 4,5 (quatro vírgula cinco) milhões de requisições por segundo na camada 7 do modelo OSI;

1.7.6. Suportar, no mínimo, 75 (setenta e cinco) Gbps de throughput para tráfego SSL/TLS;

1.7.7. Suportar, no mínimo, 90.000 (noventa mil) transações SSL por segundo, considerando cifras ECDHE-ECDSA P-256;

1.7.8. Suportar, no mínimo, 115.000 (cento e quinze mil) transações SSL por segundo, considerando cifras com certificado RSA e chaves de 2.048 bits;

1.7.9. Suportar, no mínimo, 80 (oitenta) Gbps de compressão;

1.7.10. Suportar, no mínimo, 160 (cento e sessenta) milhões SYN Cookies/segundo;

1.7.11. Suportar, no mínimo, 5 (cinco) milhões de respostas por segundo de consultas de DNS;

1.7.12. Suportar, no mínimo, 24 (vinte e quatro) instâncias virtuais isoladas entre si, com sistema operacional, plano e controle e plano de dados próprios, inclusive de versões diferentes, e reserva de recursos;

1.7.13. Possuir, no mínimo, 16 (dezesseis) portas 10/25 Gigabit Ethernet SFP+/SFP28, devendo ser acompanhado de 8 (oito) adaptadores 10GBase-SR e 8 (oito) adaptadores 25GBase-SR para fibras multimodo com conectores do tipo LC;

1.7.14. Possuir, no mínimo, 4 (quatro) portas 40/100 Gigabit Ethernet QSFP+/QSFP28, devendo ser acompanhado de 2 (dois) adaptadores 40GBase-SR4 e 2 (dois) adaptadores 100GBase-SR4 para fibras multimodo com conectores do tipo MPO;

1.7.15. Possuir, no mínimo, 1 porta de gerenciamento Ethernet 1000BASE-T out-of-band;

1.7.16. Possuir, no mínimo, 1 porta USB 3.0;

1.7.17. Possuir, no mínimo, 1 porta de console serial;

1.7.18. Possuir, no mínimo, 2 discos SSD configurados em RAID-1;

1.7.19. Suportar agregação de portas baseado no protocolo LACP, em modo passivo e ativo, com pelo menos 8 portas em um mesmo conjunto agregado;

1.7.20. Suportar a Spanning-Tree (802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s);

1.7.21. Suportar 802.1q para o transporte de múltiplas VLAN por uma única porta e por um conjunto agregado de portas;

1.7.22. Permitir configurar, pelo menos, 2.000 (duas mil) VLANs;

2. Requisitos gerais do componente software de gerenciamento e licenciamento da expansão tecnológica (ADC)

2.1. Suportar IPv4 e IPv6;

2.2. Suportar múltiplas tabelas de roteamento independentes em IPv4 e IPv6;

2.3. Suportar VXLAN para integração com o ambiente de virtualização;

2.4. Suportar configuração de endereçamento IP estático e dinâmico (DHCP/BOOTP) para o gerenciamento;

2.5. Suportar implementação em alta disponibilidade,

2.5.1. Implementar modo ativo/standby, com equipamento da mesma marca e modelo;

2.5.2. Suportar modo ativo/ativo para, pelo menos, as funções de balanceamento de servidores. Aceita-se como ativo/ativo a utilização de dois endereços virtuais, onde cada endereço fica ativo em um elemento e standby no outro;

2.5.3. Permitir a sincronização das configurações de forma automática e manual, forçando a sincronização quando necessário;

2.5.4. Permitir utilizar qualquer endereçamento IP, inclusive os definidos na RFC 1918, para criação de cluster, hearbeat e sincronização entre os equipamentos;

2.5.5. Fornecer todos os recursos de redundância da solução sem nenhuma despesa com licenças adicionais;

2.5.6. Permitir expansão do cluster adicionando novos equipamentos inclusive de modelos diferentes;

2.6. Possuir interface gráfica via web e interface via CLI por SSH e console para administração, gerenciamento e monitoramento do equipamento;

2.6.1. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

2.6.2. Permitir habilitar e desabilitar acesso administrativo via SSH por qualquer interface do equipamento;

2.6.3. Manter internamente múltiplos arquivos de configurações do sistema;

2.6.4. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e sistema operacional;

2.6.5. Possuir recurso de autocompletar nos comandos na CLI, com ajuda contextual;

2.6.6. Permitir a configuração de múltiplas contas locais de administradores;

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

2.6.8. Possuir, no mínimo, três níveis de usuários na GUI: administrador, analista e somente-leitura;

2.6.9. Suportar autenticação e autorização externa de usuários administradores através de RADIUS, LDAP, Active Directory e TACACS+;

2.6.10. A interface gráfica deve permitir a atualização do sistema operacional, atualização de componentes e instalação de patches;

2.6.11. Permitir selecionar pela interface gráfica a versão do sistema operacional para inicialização do equipamento;

2.6.12. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);

2.6.13. Suportar a rollback de configuração e imagem;

2.6.14. Possuir o registro local de eventos relevantes do sistema e suportar o envio via syslog de eventos relevantes ao sistema, com capacidade de configuração de múltiplos servidores de syslog;

2.6.15. Implementar rate limit da taxa logs enviados para servidores externos, com o objetivo de prevenir a sobrecarga e perda de logs por motivos de alta utilização de CPU, memória ou uso de banda;

2.6.16. Permitir reiniciar o equipamento pela interface gráfica e por CLI;

2.6.17. Implementar SNMPv1, SNMPv2c e SNMPV3;

2.6.18. Implementar traps SNMP;

2.6.19. Permitir a criação de MIBs customizadas;

2.6.20. Possuir suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events

2.6.21. Possuir agente integrado de coleta e exportação de métricas de desempenho e eventos:

2.6.21.1. Coleta de métricas de desempenho compatível com Prometheus;

2.6.21.2. Coleta de métricas de desempenho em formato JSON utilizando cliente HTTP;

2.6.21.3. Exportação de métricas de desempenho compatíveis com, pelo menos, os sistemas AWS CloudWatch e S3, Azure Log Analytics e Application Insights, DataDog, ElasticSearch, Fluentd, GCP Cloud Monitoring e Logging, Graphite, Kafka, OpenTelemetry, Splunk e StatsD;

2.6.21.4. Exportação de métricas de desempenho em formato JSON para um servidor HTTP;

2.6.21.5. Permitir definir critérios de inclusão e exclusão de coleta e exportação de métricas;

2.6.21.6. Deve incluir métricas de desempenho relacionadas a servidores virtuais, pool e pool members;

2.6.21.7. Deve incluir métricas de throughtput, conexões, bits, pacotes, disponibilidade;

2.6.21.8. Deve incluir métricas de requisições, respostas;

2.6.21.9. Deve incluir métricas de criptografia, incluindo cifras, algoritmos, versão, conexões, bytes criptografados, bytes descriptografados;

2.6.21.10. Deve incluir métricas de certificados digitais, incluindo data de expiração, issuer e subject;

2.6.21.11. Deve incluir métricas relacionadas a CPU, memória, discos e interfaces;

2.6.21.12. Deve incluir métricas de desempenho dos scripts de manipulação de tráfego, incluindo total de execuções, média de ciclos, máximo e mínimo de ciclos e falhas;

2.6.21.13. Deve incluir informações de inventário (hostname, id, versão, localização, plataforma, chassi, módulos provisionados);

2.6.21.14. Deve incluir métricas do cluster, incluindo data de sincronização;

2.6.21.15. Deve incluir informações de data da última configuração aplicada;

2.6.21.16. Deve possuir documentação pública do fabricante contendo informações de configurações, exemplos de configuração e modelos de mensagens;

2.6.22. Implementar debugging utilizando CLI via console e SSH;

2.6.23. Possuir ferramenta interna de captura de tráfego de rede com informações contextuais da solução inseridas em cada pacote/frame;

2.6.24. Permitir a exportação de informações de diagnóstico, logs, configurações, desempenho para análises externas sem interferência na solução em produção. A análise deve ser feita em ferramenta, disponível sem custo adicional, online via web ou via aplicação para Windows, Linux ou MacOS;

2.6.25. Deve possuir suporte a Link Layer Discovery Protocol (LLDP), com, pelo menos, as informações: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size

2.6.26. Suportar exportação de informações de fluxos através sFlow, NetFlow, IPFIX ou outro protocolo similar;

2.6.27. Permitir a criação de códigos ou scripts capazes de manipular o tráfego, incluindo descartar, redirecionar, alterar, substituir e comparar valores e atributos, a partir de informações extraídas da conexão, sessão e protocolos;

2.6.27.1. Permitir utilizar listas de dados como fonte de dados por um script para validar se as conexões a serem estabelecidas obedecem a um dos critérios contidos nessa base de dados;

2.7. Implementar roteamento IPv4 e IPv6 estático e dinâmico;

2.7.1. Suportar a criação de múltiplos domínios de roteamento, com tabelas de rotas isoladas, em IPv4 e IPv6, BGP, OSPF e RIP em IPv4 e IPv6;

2.7.2. Permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;

2.7.3. Suportar integração via BGP para divulgação de prefixos;

2.7.4. Deve garantir que o retorno do tráfego seja encaminhado para o mesmo host que enviou o tráfego inicialmente para a solução, independente da configuração de rotas do equipamento. Por exemplo, no caso de múltiplos roteadores com acesso à Internet, a solução deve enviar o tráfego de retorno para o cliente sempre para o mesmo roteador que encaminhou o tráfego do cliente inicialmente para a solução;

2.7.5. Suportar Equal Cost Multipath (ECMP);

2.7.6. Implementar Bidirectional Forward Detection (BFD);

2.8. Implementar funções de entrega de aplicações através do balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;

2.8.1. Suportar os protocolos HTTP/1.0, HTTP/1.1, HTTP/2 e HTTP/3, para comunicação com o cliente e comunicação com o servidor;

2.8.2. Implementar a reutilização de conexões entre a solução e os servidores, para diferentes clientes e diferentes requisições;

2.8.3. Suportar os métodos de balanceamento round robin, least connections, weighted (por peso), tempo de resposta mais rápida baseado no tráfego real, baseado em parâmetros dinâmicos coletados via SNMP ou WMI;

2.8.4. Implementar criptografia de cookies;

2.8.5. Implementar persistência com pelo menos os métodos por cookie inserindo um novo cookie na sessão, por cookie utilizando um valor do cookie da aplicação, sem adição de cookie, por endereço IP destino, por endereço IP origem, por sessão SSL, parâmetros da URL acessada, parâmetro no header HTTP, qualquer informação do payload camada 7;

2.8.6. Permitir configuração de grupos de servidores secundários que devem ser utilizados para balanceamento somente quando uma quantidade mínima especificada de servidores estiver disponível no grupo primário. Caso o número de servidores disponíveis fique menor do que o especificado, a solução deve automaticamente distribuir o tráfego para o próximo grupo. Caso o número de servidores disponíveis volte ao valor mínimo, a solução deve automaticamente voltar a utilizar o grupo primário de

servidores;

2.8.7. Permitir a replicação do tráfego destinado a servidores virtuais, permitindo habilitar a cópia do tráfego entre o cliente e a solução e entre a solução e o servidor;

2.8.8. Implementar pelo menos monitores de servidores de servidores via ICMP, conexões TCP e UDP pela respectiva porta no servidor e HTTP e HTTPS, incluindo HTTP/2;

2.8.9. Suportar balanceamento de carga de servidores SIP para VoIP;

2.8.10. Permitir limitar o número de conexões estabelecidas com cada servidor real;

2.8.11. Permitir limitar o número de conexões estabelecidas com cada servidor virtual;

2.8.12. Implementar Network Address Translation (NAT) do IP do servidor;

2.8.13. Implementar Network Address Translation (NAT) do IP do cliente;

2.8.14. Implementar proteção contra Denial of Service (DoS) em camada 3, 4 e 7;

2.8.15. Implementar proteção contra SYN floods;

2.8.16. Suportar servidores virtuais com endereço IPv4 e os servidores reais com endereços IPv6;

2.8.17. 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;

2.8.18. Suportar Stream Control Transmission Protocol (SCTP);

2.8.19. Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados assistida por hardware especializado.

2.8.19.1. Permitir recriptografar a conexão entre a solução e o servidor;

2.8.19.2. Permitir espelhamento de tráfego de conexões TLS;

2.8.19.3. 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;

2.8.20. Em relação ao tráfego TLS, deve suportar:

2.8.20.1. Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;

2.8.20.2. Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;

2.8.20.3. Autenticação mútua (mTLS), quando ambas as autenticações acima mencionadas ocorrem. Durante a autenticação com mTLS, a solução deve apresentar para o servidor um certificado de cliente com atributos extraídos do certificado original obtido do cliente, preservando a autenticação mútua fim a fim;

2.8.20.4. Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;

2.8.20.5. Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente;

2.8.21. Suportar os algoritmos para sessões TLS:

2.8.21.1. SSL session cache Timeout;

2.8.21.2. Session Ticket;

2.8.21.3. OCSP (Online Certificate Status Protocol) Stapling;

2.8.21.4. Dynamic Record Sizing;

2.8.21.5. ALPN (Application Layer Protocol Negotiation);

2.8.21.6. Perfect Forward Secrecy;

2.8.22. Implementar limpeza de cabeçalho HTTP;

2.8.23. Implementar compressão de conteúdo HTTP, suportar os algoritmos gzip e deflate e permitir definir compressão especificamente para certos tipos de objetos;

2.8.24. Permitir a criação de políticas para classificação de tráfego através de parâmetros da aplicação, incluindo informações de geolocalização IP, cabeçalhos de autenticação HTTP, cookies e operações de cookie, cabeçalhos HTTP, host, método, Referer, Status Code e URI;

2.8.25. Permitir as ações para o tráfego classificado bloqueio, reescrita e manipulação de URL, adicionar cabeçalho HTTP, redirecionar o tráfego para um servidor específico, escolher uma política de proteção web, logging do tráfego;

2.8.26. Suportar log de todas as sessões, incluindo endereço IP de origem, Porta TCP e UDP de origem, endereço IP de destino, porta TCP e UDP de destino, protocolo de camada 4 (TCP ou UDP), data e hora da mensagem, URL acessada;

2.8.27. Permitir utilizar diferentes configurações de envio de eventos de uma mesma aplicação, de forma que eventos válidos sejam enviados para um servidor e eventos de violações de segurança sejam enviados para outro servidor;

2.8.28. Permitir exportar eventos de acesso para servidores externos com configuração das informações exportadas;

2.8.29. Permitir a configuração de autenticação e autorização de clientes HTTP, através de base LDAP, RADIUS e certificados digitais;

2.8.30. Implementar integração com ambientes de orquestração de containers para criação dinâmica de serviços de entrega de aplicações e balanceamento de carga através dos serviços, modificando a configuração com base em mudanças feitas no ambiente;

2.8.30.1. Suportar, pelo menos, as plataformas Kubernetes “Vanilla”, Red Hat OpenShift e VMware Tanzu;

2.8.30.2. Permitir a configuração através de ConfigMaps e CustomResourceDefinition (CRD);

2.8.30.3. O ADC deverá receber em tempo real as alterações do ambiente e atualizar automaticamente o pool de pods disponíveis para o serviço publicado;

2.9. Implementar proteção de aplicações no nível de rede e protocolo;

2.9.1. Permitir implementação no modo que todo o tráfego seja bloqueado com exceções explícitas em regras de permissões e no modo que todo tráfego é permitido com exceções explícitas em regras de bloqueio;

2.9.2. Proteger de ataques DDoS nas camadas de rede e de sessão, com mitigação assistida por hardware;

2.9.3. Proteger de ataques DDoS que utilizem SSL;

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

2.9.4.1. Endereço IP de destino

2.9.4.2. Endereço IP de origem

2.9.4.3. Porta de destino

2.9.4.4. Porta de origem

2.9.4.5. VLAN

2.9.4.6. Protocolo

2.9.4.7. Ação

2.9.4.8. Horário

2.9.4.9. Log;

2.9.4.10. Permitir definir agendamento para ativação da regra;

2.9.4.11. Permitir criar regras com base em zonas de segurança e por interface ou VLAN;

2.9.5. Implementar a descoberta automática de serviços presentes em objetos monitorados;

2.9.6. Permitir definir, no mínimo, as seguintes ações no tráfego:

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

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

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

2.9.7. Deve ser possível criar regras que sejam aplicadas em diferentes hierarquias, incluindo, no mínimo:

2.9.7.1. Global, regras válidas para todo o tráfego;

2.9.7.2. Domínio de roteamento, regras válidas para todo o tráfego daquele domínio;

2.9.7.3. Objeto, regras válidas para objetos específicos;

2.9.8. Deve possuir criptografia IPSEC para comunicação entre sites;

2.9.9. Permitir a configuração de alertas que informem automaticamente sobre ataques e anomalia de tráfego, através de limiares baseados no perfil de rede ou através de limites de tráfego atingido;

2.9.10. Permitir a restauração das configurações de proteções originais;

2.9.11. Deve permitir criar lista de exceção de regras por endereço IP específico ou faixa de sub-rede;

2.9.12. Permitir a criação de códigos ou scripts para customizar e aumentar o nível de segurança contra DDoS;

2.9.13. Permitir o consumo de listas externas de IPs para bloqueio com base em destino e origem, com atualização automática e ajuste manual da frequência de atualização;

2.9.14. Permitir o acionamento via API do descarte de conexões (shun) para integração com terceiros, tais como SIEM, IPS, IDS e outros;

2.9.15. Permitir a criação de regras de filtragem através de API REST declarativa;

2.9.15.1. A documentação da API deve ser pública;

2.9.16. Exibir uma lista de proteções ativas juntamente com estatísticas resumidas sobre as quantidades de tráfego descartado e aceito

2.9.17. Incluir informações estatísticas sobre o tráfego total e o total bloqueado por cada tipo de prevenção;

2.9.18. Implementar proteção contra pacotes inválidos, incluindo verificação para DNS malformed, Bad ICMP Frame, Bad ICMP Checksum, ICMP Frame too Large, BadIGMP Frame, Bad IP TTL Value, Bad IP Version, Header Length Too Short, Bad Source, Bad IPV6 Hop Count, Bad IPV6 Version, Bad TCP Checksum, Bad TCP Flags, SYN & FIN Set, Bad UDP Checksum, ARP Flood, ICMPv4 Flood, ICMPv6 Flood , IGMP Flood, IGMP Fragment Flood, TCP RST Flood, TCP SYN ACK Flood, TCP SYN Flood, UDP Flood, SIP ACK Method, SIP Malformed, Single Endpoint Flood, Single Endpoint Sweep, LAND Attack, DNS Water-torture e fornecer estatísticas para os pacotes descartados;

2.9.19. Implementar descarte de sessões TCP ociosas se o cliente não enviar uma quantidade de dados dentro de um período configurável;

2.9.20. Limitar o número de consultas DNS por segundo através da configuração de limiares;

2.9.21. Mitigar, no mínimo, os tipos de ataques ICMP/UDP/TCP Flood, TCP Flag Abuse, GET/POST Flood, SYN Flood, UDP Bandwidth Attack, Smurfing, NTP Reflection Attack, TCP/UDP Bandwidth Attack, Fragging Attack, Slowloris, Connection Attack e Fragmentation Attacks;

2.9.22. Suportar envio de SNMP traps para cada ataque DoS detectado;

2.9.23. Possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes;

2.9.24. Deve possuir a funcionalidade de limiares automático para vetores de DoS:

2.9.25. Essa funcionalidade deve valer tanto para proteção do equipamento como também para proteção de serviços específicos.

2.9.26. Os limiares automáticos serão construídos pelo próprio sistema e aplicados aos diversos vetores de ataques selecionados;

2.9.27. Permitir configurar o sistema para detectar e mitigar assinaturas dinâmicas, capaz de detectar possíveis ameaças de DoS baseado no histórico e comportamento do tráfego e mitigar automaticamente essas ameaças;

2.9.28. Suportar integração com serviço de proteção de DDoS em nuvem, com compartilhamento de informação de vetores, através da sinalização de ataques em andamento para redirecionamento de tráfego via BGP e limpeza do tráfego em centros de limpezas externos, independente do provedor local de serviços de Internet;

2.10. Implementar serviços de entrega de aplicações distribuídas através do serviço de DNS;

2.10.1. Implementar serviços de DNS com as funções de DNS autoritativo, DNS secundário, DNS resolver, DNS cache e balanceamento de servidores de DNS;

2.10.2. Implementar DNSSec, independente da estrutura dos servidores DNS em uso;

2.10.3. Implementar transferência de zonas para múltiplos servidores DNS primários responsáveis por diferentes zonas;

2.10.4. Suportar uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

2.10.5. Implementar offload dos servidores de DNS, funcionando como o DNS secundário;

2.10.6. Implementar proteções contra-ataques DNS, incluindo no mínimo a inspeção de protocolo, validação de protocolo, UDP flood, pacotes malformados, teardrop e DNS Water-torture;

2.10.7. Permitir a criação de códigos ou scripts que possam manipular as respostas de DNS;

2.10.8. Implementar filtragem de pacotes e tipos de requisições;

2.10.9. Implementar segurança do protocolo DNS, protegendo de ataques de negação de serviço, NXDOMAIN, reflexão e amplificação de DNS e Cache Poisoning;

2.10.10. Implementar stateful inspection das requisições e respostas de DNS;

2.10.11. Possuir base de geolocalização IP;

2.10.12. Implementar DNS64 e implementar as seguintes integrações:

2.10.12.1. Cliente envia consulta AAAA, a solução encaminha a consulta (recursivo) com A e AAAA e responde com um prefixo + A e AAAA

2.10.12.2. Cliente envia consulta AAAA, a solução encaminha a consulta (recursivo) com A, caso não tenha resposta, faz a consulta com AAAA, responde para o cliente um prefixo + A e AAAA

2.10.12.3. Cliente envia consulta AAAA, a solução encaminha uma consulta (recursivo) como A e responde um prefixo + AAAA

2.10.13. Implementar filtros para tipos de requisição, de forma que apenas as operações e requisições autorizadas sejam encaminhadas para os servidores de DNS.

2.10.14. Suportar pelo menos os tipos de requisição SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV e TXT;

2.10.15. Suportar DNS over HTTPS (DoH);

2.10.16. Permitir a criação de resoluções de DNS com tratamento diferenciado de consultas conforme origem das requisições;

2.10.17. Apresentar estatísticas sobre consultas de DNS por aplicação, nome da query, tipo da query, endereço IP do cliente;

2.10.18. Implementar modo inline na estrutura de DNS existente e transparente;

2.10.19. Suportar IP Anycast;

2.10.20. Implementar alta disponibilidade sem depender de BGP ou outro protocolo de roteamento;

2.10.21. Implementar alta disponibilidade de Data Centers e serviços baseada em respostas a requisições DNS, de forma que a resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;

2.10.22. Suportar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;

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

2.10.24. Suportar monitores utilizando HTTPS, incluindo a validação do SNI;

2.10.25. Suportar pelo menos os algoritmos de balanceamento Round Robin, Global Availability, Ratio, LDNS Persist, Geografia, round trip time e hops;

2.10.26. Implementar persistência da conexão do usuário entre aplicações ou data centers;

2.10.27. Suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;

2.10.28. Permitir que as políticas sejam configuradas individualmente por aplicação que será balanceada;

2.10.29. Permitir que a contingência seja automática;

2.10.30. Permitir o retorno do Data Center de forma automática e manual;

2.10.31. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requisições AAAA);

2.10.32. Possuir suporte a IPv6 no balanceamento global entre datacenters;

2.10.33. Possuir a funcionalidade de resposta rápida a requisições de DNS, permitindo respostas mais rápidas para zonas que seja autoritativo;

2.10.34. Suportar Response Policy Zones (RPZ), mecanismo de proteção de resolução para DNS recursivo que permite o tratamento customizado da resolução de nomes, capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas;

2.10.35. Suportar EDNS-Client-Subnet (ECS) para tanto responder requisições de clientes para balanceamento de Data Center ou encaminhar requisições de clientes.

2.10.36. Implementar a utilização da subnet do cliente presente no ECS para tomada de decisão de balanceamento de Data Center, independente do endereço do LDNS;

2.10.37. Suportar inserir o ECS para outros servidores DNS;

2.10.38. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver, deve ser usada a persistência existente para manter o cliente no mesmo Data Center;

2.10.39. Permitir consultar a resposta de uma resolução de DNS em uma base de IP e permitir que a resposta seja alterada antes de ser enviada para o cliente;

2.10.40. Registrar todas as tentativas de comunicação com os nomes de domínio que hospedem conteúdo malicioso, incluindo IP de origem, destino, data e hora do acesso.

2.10.41. Suportar, no mínimo, as ações de apenas registrar, bloquear o dado ou substituir o nome do domínio;

2.10.42. Permitir configurar rate limit realizadas via TCP ou UDP por FQND;

2.10.43. Permitir configurar rate limit para consultas realizadas via TCP ou UDP por IP de origem;

2.11. Implementar funções de orquestração inteligente de tráfego criptografado

2.11.1. Implementar a terminação de conexões TLS entre o cliente a solução, redirecionamento inteligente do tráfego descriptografado por uma cadeia de serviços configurável e o estabelecimento de uma nova conexão TLS entre a solução e o destino do serviço;

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

2.11.3. Não deve exigir uma topologia tradicional de "ligação em cascata" dos dispositivos de segurança, em que o tráfego precisa sempre necessariamente passar por todos os dispositivos de segurança;

2.11.4. Permitir o direcionamento do tráfego descriptografado para dispositivos de segurança baseado em políticas;

2.11.5. Permitir a criação de múltiplas cadeias de serviços para diferentes tipos de análises de segurança;

2.11.6. A integração com dispositivos de segurança deve ser independente de marca ou modelo, ou seja, deve ser compatível com produtos de diversos fabricantes como Cisco, Check Point, FireEye, Fortinet, McAfee, Palo Alto, dentre outros e de forma genérica dispositivos em camada 3 e espelhamento de tráfego;

2.11.7. Deve monitorar cada dispositivo de segurança independentemente, implementando a configuração de política para realizar o bypass do dispositivo indisponível e interrupção do tráfego;

2.11.8. Permitir a resiliência dos serviços dentro da zona de inspeção, inclusive fazendo o balanceamento de carga entre múltiplos equipamentos do mesmo serviço;

2.11.9. Permitir a escalabilidade independente de cada dispositivo de segurança, ou seja, caso necessário inserir, por exemplo, mais um dispositivo NGFW na zona de inspeção, a solução deve ser configurada para distribuir o tráfego entre os dispositivos NGFW ativos;

2.11.10. Permitir escalar os dispositivos de segurança com alta disponibilidade, usando monitores de disponibilidade para identificar o estado de cada equipamento de segurança;

2.11.11. Permitir que múltiplos equipamentos de segurança de diversos fabricantes tenham visibilidade tanto do tráfego de entrada, fazendo que eles continuem realizando suas inspeções procurando por malwares, exfiltração de dados e imposição de políticas de segurança;

2.11.12. 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;

2.11.13. Implementar algoritmos de criptografia em hardware específico;

2.11.14. Suportar, pelo menos, os protocolos IMAP, SMTPS, POP3, FTP e HTTP, incluindo HTTP/2;

2.11.15. Suportar, pelo menos, as topologias de integração como proxy explícito, proxy transparente, em linha em camada 3 e proxy reverso;

2.11.16. Tratar todo o tráfego encaminhado para a solução, funcionando como um roteador na rede, realizando a interceptação do TLS apenas de endereços configurados;

2.11.17. Permitir a configuração de IPs e portas específicos para interceptação do tráfego TLS;

2.11.18. Permitir utilizar diferentes servidores de DNS por topologia de integração;

2.11.19. Suportar ações caso o certificado original do servidor expire;

2.11.20. Suportar ações caso o certificado original do servidor não seja confiável;

2.11.21. Suportar bypass do tráfego caso falhe o TLS handshake;

2.11.22. Suportar o envio de tráfego para dispositivos independente da conexão física, ou seja, não deve exigir que o dispositivo de segurança esteja diretamente conectado a solução;

2.11.23. Suportar o envio de tráfego ICAP para dispositivos;

2.11.24. Suportar enviar tráfego para dispositivos passivos, como DLPs;

2.11.25. Suportar web proxy dentro da camada de inspeção, incluindo HTTP/2;

2.11.26. Suportar fazer o offload da autenticação na solução de visibilidade SSL e encaminhar o usuário autenticado para o serviço de web proxy;

2.11.27. Deve ser compatível com aplicações que utilizam mTLS (mutual TLS), como API entre sistemas e aplicações com autenticação do usuário via certificado, ou seja, a solução deve ser capaz de autenticar o cliente utilizando o certificado de servidor e se autenticar com o servidor utilizando um certificado de cliente, enviando o tráfego descriptografado para os dispositivos de segurança para inspeção, de forma que o servidor possa identificar o cliente;

2.11.28. Implementar balanceamento de tráfego entre dispositivos de inspeção;

2.11.29. Implementar o balanceamento de servidores após o retorno do tráfego pela cadeia de inspeção, ou seja, uma conexão inbound que foi interceptada, inspecionada na zona de segurança, ao reestabelecer a criptografia, deve ser balanceada entre servidores reais;

2.11.30. Suportar enviar o tráfego original para dispositivos de inspeção;

2.11.31. Suportar mais de 10 dispositivos;

2.11.32. Suportar fazer bypass ou aplicar uma cadeia de serviço para inspeção com base na classificação e categoria do certificado/site;

2.11.33. Deve implementar a renegociação de sessão SSL/TLS;

2.11.34. Permitir utilizar métodos de classificação como por exemplo URL, geolocalização, domínio, IP origem, IP destino, porta e protocolo para definir se o tráfego deve ser bloqueado, descriptografado e enviado para um serviço ou outro e realizar o bypass desse tipo de tráfego;

2.11.35. Suportar a alteração/tradução de portas para o tráfego descriptografado que permita que os dispositivos de segurança identifiquem um tráfego em texto claro para a devida inspeção, por exemplo alterar a porta de TCP de 443 (HTTPS) para 80 (HTTP);

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

2.12. Implementar proteção para aplicações web e API contra ameaças na camada de aplicação;

2.12.1. Possuir tecnologia para mitigação de DDoS em camada 7 a partir de análises comportamentais;

2.12.2. Implementar ajustes automáticos e adaptativos de limiares de DoS;

2.12.3. Permitir a captura automática do tráfego relativo a ataques DoS em camada 7, web scraping e força bruta;

2.12.4. Implementar proteção para aplicações web contra ameaças listadas no OWASP Top 10 2021;

2.12.5. Implementar modelo positivo de segurança de aplicações web;

2.12.6. Implementar modelo negativa de segurança, ou seja, adotar assinatura de ataques, ameaças e exploração de vulnerabilidade, de aplicações web;

2.12.7. Possuir conjuntos de configurações de segurança pré-definidas para configuração rápida de políticas;

2.12.8. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

2.12.9. Permite 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;

2.12.10. Permitir a integração com firewall de banco de dados;

2.12.11. Suportar aplicações que utilizam protocolo WebSocket;

2.12.12. Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0, para comunicação com o cliente e comunicação com o servidor, sem a necessidade de downgrade de versão;

2.12.13. Implementar proteção contra:

2.12.13.1. Acesso por força bruta;

2.12.13.2. DoS e DDoS em camada 7;

2.12.13.3. Buffer Overflow;

2.12.13.4. Cross Site Request Forgery (CSRF);

2.12.13.5. Cross-Site Scripting (XSS);

2.12.13.6. Server-Side Request Forgery (SSRF);

2.12.13.7. SQL Injection;

2.12.13.8. Parameter tampering;

2.12.13.9. Cookie poisoning;

2.12.13.10. HTTP Request Smuggling;

2.12.13.11. Manipulação de campos escondidos (hidden input);

2.12.13.12. Manipulação de cookies;

2.12.13.13. Roubo de sessão através de manipulação de cookies;

2.12.13.14. Sequestro de sessão;

2.12.13.15. Validação de consistência de formulários;

2.12.13.16. Validação do cabeçalho do "user-agent" para identificar clientes inválidos;

2.12.14. Permitir especificar quais URLs devem ser utilizadas para proteção contra CSRF (Cross-Site Request Forgery);

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

2.12.16. Suportar HTTP Batched Request com proteções e assinaturas considerando individualmente URIs, cabeçalhos e conteúdo;

2.12.17. Suportar codificação fragmentada (chunked encoding);

2.12.18. Suportar validações de protocolo:

2.12.18.1. Restrição de métodos;

2.12.18.2. Restrição de protocolos e versões;

2.12.18.3. Validação de conformidade com RFCs;

2.12.18.4. Validação de caracteres URL-encoded;

2.12.18.5. Validação de codificação fora de padrão %uXXYY.

2.12.19. Suportar validações de HTML com nome de parâmetros, tamanho e tipo dos valores de parâmetros e combinação de nome, tipo e tamanho de parâmetros;

2.12.20. Suportar as técnicas de detecção:

2.12.20.1. URL-decoding;

2.12.20.2. Terminação Null Byte String;

2.12.20.3. Paths autorreferenciados;

2.12.20.4. Case de caracteres misturados;

2.12.20.5. Uso excessivo de espaços em branco;

2.12.20.6. Decodificação de entidades HTML;

2.12.20.7. Caracteres de escape;

2.12.21. Suportar POST para upload de arquivo e permitir configurar restrições para tamanho individual de arquivo;

2.12.22. Permitir a inspeção externa de arquivos enviados por usuários (upload) para os servidores de aplicação utilizando Internet Content Adaptation Protocol (ICAP);

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

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

2.12.25. Implementar validação de URL;

2.12.26. Validação de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT) por URL;

2.12.27. Implementar proteção de aplicações web que utilizam chamadas de API, protegendo tanto a aplicação como a API, com a visibilidade que se trata da mesma sessão de usuário;

2.12.28. Suportar o uso de páginas de login que utilizam AJAX;

2.12.29. Permitir a customização da resposta de bloqueio;

2.12.30. Permitir a configuração de lista de exceções temporárias ou permanentes de endereços IP bloqueados;

2.12.31. Permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem limites estabelecido, por um período configurável;

2.12.32. Implementar as proteções:

2.12.32.1. Proteção contra exposição de informações do ambiente e servidores internos como, sistema operacional e servidor web;

2.12.32.2. Ocultar qualquer mensagem de erro HTTP dos usuários;

2.12.32.3. Remover as mensagens de erro às páginas que serão enviadas aos usuários;

2.12.33. Permitir a configuração da página de bloqueio;

2.12.34. Suportar políticas por geolocalização para restrição de acesso a determinados países;

2.12.35. Implementar aprendizado automático para identificação da estrutura da aplicação, incluindo URLs, parâmetros URLs, campos de formulários, tipo de dado, tamanho de caracteres, cookies;

2.12.36. O aprendizado deve ser capaz de diferenciar atributos com o mesmo nome, mas presentes em URLs diferentes;

2.12.37. Implementar aprendizado automático de XML;

2.12.38. Permitir a importação de arquivo de esquema XML;

2.12.39. Implementar aprendizado automático de JSON;

2.12.40. Permitir a importação de arquivo de esquema JSON;

2.12.41. Permitir a criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real;

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

2.12.43. Implementar detecção e mitigação de ameaças e ataques com base em assinaturas de ataques, com atualização periódica e automática da base de assinaturas;

2.12.44. As assinaturas devem ser atualizadas durante o período do contrato, sem custo adicional;

2.12.45. Não serão aceitas soluções que definem assinaturas como sendo uma base de reputação de IP;

2.12.46. A atualização deve ser relacionada apenas as assinaturas, não sendo aceitas soluções que demanda a atualização do sistema operacional para atualização de cada nova versão da base de assinaturas;

2.12.47. Permitir a configuração automática de assinaturas com base em uma lista interna de tecnologias utilizadas pela aplicação;

2.12.48. Permitir desabilitar assinaturas específicas para determinados parâmetros, se comportando como exceção da configuração geral da política;

2.12.49. Permitir configurar um período de adaptação de novas assinaturas, quando nenhuma requisição que viole a assinatura deve ser bloqueada, apenas informada em relatório. Este processo deve ser automático, não sendo necessário a criação de regras específicas a cada atualização de assinatura;

2.12.50. Possuir assinaturas de ataques para conteúdo em JSON e XML;

2.12.51. Possuir proteções contra XML Bomb;

2.12.52. Possuir proteção para WebServices, suportar WS-I Basic Profile, importação de WSDL e aplicação de controles, criptografar e descriptografar partes das mensagens SOAP, assinar digitalmente e verificar de partes das mensagens SOAP;

2.12.53. Possuir integração com soluções externas de análise vulnerabilidade para importação de relatórios e configuração de políticas de segurança, indicando quais vulnerabilidades podem ser resolvidas e quais devem ser resolvidas manualmente externamente;

2.12.54. Implementar detecção de DoS na camada 7, através de análise comportamental, com aprendizado automático do comportamento da aplicação e combinação com nível de carga do servidor;

2.12.54.1. Permitir apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

2.12.54.2. Implementar detecção com base no número de requisições por segundo enviados a uma URL específica;

2.12.54.3. Implementar detecção com base no número de requisições por segundo enviados de um IP específico;

2.12.54.4. Implementar detecção com base na validação do cliente através de código executado no navegador para identificação de bots;

2.12.54.5. Implementar detecção com base no aumento de um determinado percentual do número de transações por segundo (TPS);

2.12.54.6. Implementar detecção com base no aumento de carga e processamento do servidor de aplicação;

2.12.54.7. Implementar detecção com base no número máximo de transações por segundo de um determinado IP;

2.12.55. Implementar mitigações para ataques DoS, incluindo resolução de CAPTCHA, descarte de todas as requisições de um determinado IP, descarte por geolocalização IP, injeção de um desafio JavaScript para detectar se é um usuário legítimo ou bots;

2.12.56. Implementar mitigação de ataques DDoS através de assinaturas dinâmicas em tempo real para proteção da aplicação;

2.12.57. Implementar detecção e mitigação de ataques de força bruta de usuário/senha em páginas de login, com configuração da quantidade máxima de tentativas e tempo de mitigação;

2.12.57.1. Identificar ataques com diferentes usuários e mesma origem;

2.12.57.2. Identificar ataques com diferentes origens e mesmo usuário;

2.12.57.3. Identificar ataques de forma global, considerando a quantidade de tentativas e implementando contramedidas de forma global para a política;

2.12.58. Possuir funcionalidade para integração com listas externas de credenciais expostas para mitigar ataques Credential Stuffing;

2.12.59. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs após validação sem sucesso de desafios e permitir a configuração do tempo de bloqueio;

2.12.60. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs que ultrapassem um número máximo de violações por minuto e permitir a configuração do tempo de bloqueio;

2.12.61. Implementar detecção e mitigação para proteção contra bots contra robôs através da combinação de desafios enviados ao navegador do usuário e técnicas avançadas de análise comportamental;

2.12.62. Não serão aceitas soluções que utilizam apenas o user-agent para detecção de bots;

2.12.63. Implementar proteção proativa contra-ataques automatizados por bots e outras ferramentas, como web scrapers.

2.12.64. Possuir atualização automática de definição de bots;

2.12.65. Permitir a configuração de bloqueio e permissão de bots benignos conhecidos, como Google, Yahoo! e Microsoft Bing,

2.12.66. Permitir a criação de definições de bots;

2.12.67. Implementar proteção de APIs através da imposição de regras de endpoint e métodos permitidos;

2.12.68. Permitir a configuração de quotas e rate limits para chamadas em APIs de forma global na política;

2.12.69. Permitir a configuração de quotas e rate limits para chamadas em APIs por endpoint;

2.12.70. Permitir configurar exceções as regras de rate limits para chamadas na API;

2.12.71. Implementar proteção de conteúdo no formato JSON (JavaScript Object Notation);

2.12.72. Suportar proteção de conteúdo de mensagens no formato GraphQL, incluindo assinaturas de ataques, profundidade de query, GraphQL batching, inspeção de conteúdo JSON em mensagens POST e GET;

2.12.73. Suportar importação de especificação de API compatível com OpenAPI v2 e v3, nos formatos YAML ou JSON, com suporte a parâmetros no path e importação de respostas;

2.12.74. Implementar funcionalidade de autenticação e autorização de clientes de API utilizando, pelo menos, os métodos HTTP Basic e OAuth 2.0;

2.12.75. Implementar funcionalidade para prevenir vazamento de informações, dados sensíveis e outros tipos de dados confidenciais, sigilosos ou restrito, através do bloqueio ou remoção dos dados confidenciais;

2.12.76. Implementar funcionalidades para prevenir vazamento de dados sensíveis em mensagens de erro HTTP, códigos das aplicações, entre outros, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários;

2.12.77. Implementar funcionalidade para ocultar erros de aplicação ou infraestrutura do usuário;

2.12.78. Permitir a configuração de fluxo de navegação da aplicação, de forma que um usuário só pode alcançar determinada URL se passar por outras anteriormente;

2.12.79. Permitir a correção de um falso positivo através da aceitação da requisição e atualização da política de forma automática;

2.12.80. Possuir um nível severidade de violação de múltiplos níveis para fácil identificação de violações de maior e menor prioridade;

2.12.81. Implementar um identificador único para cada requisição tratada pela solução;

2.12.82. Permitir o armazenamento local de eventos e exportação para servidores externos;

2.12.83. Permitir configurar a retenção dos eventos por tempo e volume;

2.12.84. Implementar a detecção, remoção ou codificação de dados sensíveis dos eventos como, por exemplo, números de cartão de crédito, CPF e senhas;

2.12.85. Implementar a criptografia de parâmetros específicos da aplicação, tais como credenciais e dados sensíveis, sem a necessidade de atualizar a aplicação. Esta criptografia de dados deve ser implementada no payload do HTTP, ou seja, nos dados propriamente ditos e não apenas via protocolo de transporte/túnel (TCP/TLS);

2.12.86. Implementar a ofuscação do nome de um parâmetro sensível da aplicação utilizando caracteres aleatórios, devendo ser mudado frequentemente pela solução para dificultar ataques direcionados;

2.12.87. Possuir API REST para configuração de servidores virtuais, políticas de segurança, parâmetros, perfis e demais configurações;

2.12.88. Permitir exportar as políticas de segurança para arquivos texto, JSON ou XML;

2.12.89. Possuir integração com esteiras de automação que permita que as configurações sejam realizadas de forma automática e dinâmica por ferramentas de automação e orquestração, permitindo que a solução seja integrada ao ciclo de desenvolvimento;

2.13. Implementar funcionalidade de gestão de tráfego de bots para detecção e mitigação de ataques automatizados, com detecção de tráfego gerado por usuários, bots benignos e malignos, através de telemetria de uso coletada da aplicação;

2.13.1. Implementar funcionalidade de forma nativa na solução ou possuir integração com serviço em nuvem do mesmo;

2.13.2. Implementar proteção de aplicações web, de dispositivos móveis e APIs;

2.13.3. Suportar a análise de, pelo menos, 5 milhões de requisições por dia entre todos os appliances da solução;

2.13.4. Deve ser capaz de identificar e classificar ações automatizadas por bots maliciosos, bots benignos e agentes humanos;

2.13.5. Implementar mecanismos para detectar técnicas avançadas e sofisticadas de automação, tais como click-farms, agentes humanos, emuladores e simuladores, “macro runners” e implementar mitigação;

2.13.6. Implementar mecanismos de análises adaptativas de comportamentos e uso das aplicações;

2.13.7. Deve suportar integração com diversos fluxos da aplicação, tais como login, criação de contas, recuperação de senha, recuperação de contas, assinaturas de newsletter, entre outros;

2.13.8. A solução não deve armazenar e processar dados pessoais, credenciais, dados digitados, payload, arquivos e informações que permitem a identificação pessoal. Será admitida a coleta e processamento do endereço IP e suas informações relacionadas, assim como o registro de teclas/caracteres funcionais;

2.13.9. Deve ser capaz de detectar e mitigar ataques de credential stuffing, account takeover, content scrapers, carding fraud, marketing fraud e inventory hoarding;

2.13.10. Deve ser capaz de detectar acesso provenientes de bots e classificar os tipos de automação utilizados;

2.13.11. Não serão aceitas soluções que dependem de CAPTCHAs para detecção e mitigação ou utilizar CAPTCHA como mecanismos de "fallback" para detecção;

2.13.12. Não serão aceitas soluções que dependem apendas de desafios ao browser via JavaScripts;

2.13.13. Para aplicações web:

2.13.13.1. Implementar a coleta de telemetria de aplicações web relacionados ao acesso e rede, ambiente e navegador, e ao comportamento e o modo de uso da aplicação no navegador e webview;

2.13.13.2. Implementar ofuscação avançada do código para prevenir técnicas de engenharia reversa;

2.13.13.3. Implementar atualizações do código de extração de telemetria para dificultar a ações de engenharia reversa;

2.13.13.4. Implementar técnicas contra tentativas de análises da telemetria coletados;

2.13.13.5. Não serão admitidas soluções que utilizam códigos JavaScript de fácil leitura;

2.13.13.6. Não serão admitidas soluções que utilizam telemetria coletados de fácil leitura;

2.13.13.7. Permitir marcação de uma transação como automatizada caso o usuário desabilite a execução de JavaScripts no navegador ou utilize extensões capazes de bloquear o JavaScript;

2.13.13.8. Permitir a criação de lista de exceções para origens conhecidas que podem desabilitar o JavaScript;

2.13.14. Para aplicativos para dispositivos móveis:

2.13.14.1. Implementar coleta de telemetria relacionados ao acesso e rede, ambiente e dispositivo, e ao comportamento e modo de uso do aplicativo nativo para dispositivos móveis através de SDK incorporado ao aplicativo;

2.13.14.2. Deve ser totalmente compatível com as políticas de publicações de aplicativos das lojas Apple App Store e Google Play Store;

2.13.14.3. Ser compatível com aplicativos Android na versão 5.x e superior (API Level 21) e aplicativos para iOS na versão 9.x e superior;

2.13.14.4. Suportar frameworks estáticos e dinâmicos de aplicativos para dispositivos móveis, tais como React, Flutter, Angular e Ionic;

2.13.14.5. Suportar integração através de ferramenta de blindagem de aplicativos para dispositivos móveis;

2.13.15. Entende-se por acesso e rede como sendo informações relacionados ao IP do usuário, tais como provedor, país, provedor de nuvem, IP residencial, número do AS e informações relacionadas, reputação do IP, e informações relacionados ao protocolo HTTP, tais como cabeçalhos HTTP, presença e ordem dos cabeçalhos HTTP, cookies, configurações de idioma, user agent, dentre outros;

2.13.16. Entende-se por ambiente, navegadores e dispositivo como sendo informações sobre plataforma onde a aplicação é consumida pelo usuário, como por exemplo o tipo do navegador, sistema operacional, hardware, versão, codificação de caracteres, resolução, fontes, plug-ins, configurações de tela, temperatura, bateria, giroscópio, orientação, data e hora, processador, dentre outros;

2.13.17. Entende-se por comportamento e modo de uso da aplicação como sendo informações relacionadas com a interação do usuário com a aplicação;

2.13.18. Deve apresentar o resultado da análise da telemetria de forma determinística, ou seja, apresentar como "sim" ou "não" para um ataque automatizado, indicando, quando disponível, o motivo ou tipo de automação detectado;

2.13.19. Possuir painéis online para visualização de eventos e estatísticas, incluindo, no mínimo:

2.13.19.1. Classificação das requisições;

2.13.19.2. Volume de requisições;

2.13.19.3. Fluxos da aplicação mais atacados;

2.13.19.4. Lista de bots maliciosos por origem IP e tipo;

2.13.19.5. Informações de origem geográfica, dispositivos e plataformas;

2.14. Implementar bases de inteligência de ameaças atualizadas automaticamente;

2.14.1. A solução deve implementar a atualização das bases de inteligência de ameaças para proteção de DoS/DDoS, serviços de DNS, de visibilidade de tráfego e de proteção de aplicações web e API durante a vigência do contrato;

2.14.2. As fontes de inteligência devem ser fornecidas diretamente pelo fabricante da solução ou parceiro homologado através de assinaturas de serviços próprios;

2.14.3. As fontes de inteligência devem ser atualizadas frequentemente pela duração do contrato sem custo adicional;

2.14.4. Deve dispor de bases de inteligência de IP, incluindo IPv4 e IPv6, classificados e categorizados em, pelo menos, as categorias fontes de ataques web, redes e hosts de botnets, scanners de websites, fontes de phishing, servidores proxies, redes e hosts que exploram vulnerabilidades em Windows, redes e hosts de negação de serviço e redes e hosts com baixa reputação;

2.14.4.1. Permitir que sejam criados filtros utilizando as categorias de IP nas funções de proteção de DDoS e serviços de DNS, de visibilidade de tráfego e de proteção de aplicações web e API;

2.14.4.2. Permitir utilizar a base de inteligência de IP durante consultas de DNS, permitir ações diferentes configuradas de acordo com a categoria e alterar a resposta antes de ser enviada para o cliente na solução de proteção de DDoS e serviços de DNS;

2.14.4.3. Permitir utilizar a base de inteligência de IP para classificar e selecionar uma cadeia de serviço na solução de visibilidade de tráfego;

2.14.4.4. Permitir que sejam criados filtros onde se verifica o endereço de origem no cabeçalho X-Forwarded-For (XFF) com base na classificação de endereços IP na solução de proteção de aplicações web e API;

2.14.5. Deve dispor de bases de inteligência de sites, classificados e categorizados em, pelo menos, armazenamento e backup pessoal, compartilhamento de arquivos p2p, dados e serviços financeiros, colaboração, instituições culturais, instituições educacionais, organizações políticas, saúde e medicina, motores de busca, e-mail corporativo, endereços IP privados, produtividade, mensagens instantâneas, download de software, religião, redes sociais (Facebook, LinkedIn, Twitter e YouTube), websites recém cadastrados, sites com exposição elevada, conteúdo suspeito, explorações recentes, DNS dinâmico, prevenção de proxy, hacking, spam, lojas de aplicativos móveis não oficiais, sites comprometidos, sites maliciosos, phishing, fraudes, spyware e adware, keyloggers, software potencialmente indesejado, botnets, links malicioso, links suspeito, iFrame malicioso, malwares para dispositivos móveis, uploads criptografados on-demand, comando e controle;

2.14.5.1. Permitir a criação de políticas de interceptação e seleção de cadeia de serviços com base em categoria do site;

2.14.5.2. Permitir a criação de regras de by-pass de interceptação com base na categoria do site ou URL;

2.14.6. Dispor de base de inteligência de ameaças relacionados a campanhas e ataques a aplicações web, correlacionando diversas fontes de inteligência e ameaças encontradas diariamente no mundo real;

2.14.6.1. As regras de proteção e assinaturas derivadas desta base de inteligência devem ser habilitadas automaticamente, sem precisar de um ciclo de aprendizagem na solução;

2.14.6.2. A base de inteligência deve implementar detecção e mitigação de ataques com baixo índice de falso-positivo;

2.14.6.3. Este serviço é complementar a atualização de assinaturas de ataques da solução de proteção de aplicações web e API, portanto, as informações disponibilizadas pela base de inteligência não devem ser limitada a apenas indicar qual assinatura do WAF for acionada, devendo disponibilizar informações contextuais incluindo, por exemplo, a capacidade de informar que um agente conhecido de ameaça usou uma exploração específica de vulnerabilidade mais recente (por exemplo, um CVE) em uma tentativa de implantação de uma ameaça como, por exemplo, um software de mineração de criptomoedas;

2.14.7. Devem ser automáticas e frequentes as atualizações de regras, políticas, configurações e demais ajustes que dependem do serviço de inteligência, sem interrupção do serviço, sem necessidade de atualização do sistema operacional e nem reiniciar o equipamento a cada atualização

2.15. Implementar painéis para monitoramento da solução;

2.15.1. Possuir relatórios do serviço de DNS incluindo tendência de latência de resposta de DNS, nomes de domínios de DNS mais requisitados, tendência de uso do cache de DNS, clientes de DNS, clientes por domínio de DNS, taxa de consultas de DNS por tipo de registro, taxa de consultas de DNS diária por servidor, pico de consultas diárias de DNS por servidor, NXDOMAIN, SERVFAIL enviados e recebidos, nomes de domínios com conteúdo malicioso, principais domínios maliciosos;

2.15.2. Possuir relatórios de proteção do serviço de DNS, incluindo eventos por período, eventos por severidade, eventos por regra, eventos por tendência e eventos por categoria;

2.15.3. Suportar a exportação de eventos de DNS utilizando IPFIX;

2.15.4. Deve possuir relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DoS;

2.15.5. Possuir relatório de ataques DDoS com indicação de início e fim do ataque;

2.15.6. Possuir relatório em tempo real sobre ataques DDoS, atualizado automaticamente;

2.15.7. Possuir relatório de ataques DDoS incluindo quantidade de eventos e severidade, ataques por protocolo, incluindo assinaturas utilizadas e serviços mais afetados;

2.15.8. Possuir relatórios de ataques DDoS incluindo a origem dos ataques, país, requisições por segundo, gatilho da proteção e mitigação adotada;

2.15.9. Suportar a exportação de eventos de DoS utilizando IPFIX;

2.15.10. Possuir painel de acompanhamento de adoção de proteções contra ameaças mais comuns, de acordo com OWASP Top 10 2021;

2.15.11. Possuir relatório de desempenho da solução, incluindo processamento total e por servidor virtual protegido;

2.15.12. Possuir relatórios consolidados de ataques incluindo, pelo menos, resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, ataques DoS, ataques de força bruta, ataques de bots, violações, URL, endereços IP, países e severidade;

2.15.13. Possuir relatório de incidentes com violações detectadas e correlacionadas, separando falsos positivos de atividades maliciosas e para facilitar a resposta a incidentes;

2.15.14. Implementar monitoração e análise de performance de aplicações web;

2.15.15. Possuir relatórios de métricas de aplicações, incluindo transações por segundo, tempo de reposta, latência do cliente e servidor, throughput de requisição e resposta e sessões;

2.15.16. Possuir relatórios de análises históricas detalhamento do tempo de resposta total de carregamento de uma URL e página e correlação de métricas de uso de rede com o comportamento das aplicações para auxiliar processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações;

2.15.17. Possuir relatórios para análise de dados por aplicações, por URL, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução;

2.15.18. Possuir relatórios para análise de estatísticas de acesso, incluindo métodos HTTP, sistema operacional e navegadores;

2.15.19. Permitir exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário

2.15.20. Possuir relatório de ataques DoS em camada 7 com indicação de início e fim do ataque;

2.15.21. Possuir relatório em tempo real sobre ataques DoS em camada 7, atualizado automaticamente;

2.15.22. Possuir relatório que permite avaliar o impacto de ataques DoS em camada 7 na performance do servidor;**2.15.23.** Possuir relatório de orquestração de tráfego, contendo, pelo menos, estatísticas sobre nomes de cifra de cliente, versões de cifra de cliente, nomes de cifra de servidor, versões de cifra de servidor, endereços IP, tipos de tráfego, status de descriptografia, ações de política, paths de serviço, categorias de URL, aplicativos, famílias de aplicativos, reputação de IP e países de destino;

ANEXO I-II - MODELO DE PROPOSTA

Razão Social:		E-mail:	CNPJ:
Endereço:	Cidade:	CEP:	Tel./Fax:

Grupo	Item	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R$)	Valor total (R$)
1	1	Renovação de garantia e licenciamento por 36 meses para appliances (ADC) F5 BIG-IP i5800	Unidade	4		
	2	Serviço de suporte técnico especializado (36 meses prorrogveis)	Meses	36		
	3	Renovação tecnológica – Instalação e configuração (por appliance - ADC) para Item 1	Unidade	4		
Valor total do Grupo 1 (R$):						

Grupo	Item	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R$)	Valor total (R$)
2	4	Componente hardware da expansão tecnológica - Appliance de alta capacidade (ADC) F5 BIG-IP r10600	Unidade	2		
	5	Componente software de gerenciamento e licenciamento da expansão tecnológica (ADC) – licenciamento e subscrições por 60 meses	Unidade	2		
	6	Garantia da expansão tecnológica – Garantia do fabricante para hardware e software (ADC) por 60 meses	Unidade	2		
	7	Instalação da expansão tecnológica – Instalação e configuração (por appliance - ADC)	Unidade	2		
Valor total do Grupo 2 (R$):						

Declarações:
i) Esta empresa declara que tem pleno conhecimento das condições necessárias para a execução do objeto.
ii) Esta empresa declara que nos preços propostos acima estão incluídas todas as despesas, frete, tributos e demais encargos de qualquer natureza incidentes sobre o objeto da contratação.
iii) Esta empresa declara estar ciente de que a apresentação da presente proposta implica na plena aceitação das condições estabelecidas no Edital e seus Anexos.
iv) Esta empresa declara estar ciente da necessidade de apresentação dos documentos de habilitação exigidos, bem como dos critérios de sustentabilidades a serem comprovados **e dos demais documentos previstos no Edital e seus Anexos.**

Validade da Proposta:
O prazo de validade desta proposta é de 60 (sessenta) dias, contados da data de abertura do Pregão.

Observações para o Preenchimento da Proposta pelas Empresas:
1) A tabela da proposta deverá ser ajustada, preenchendo-se as linhas e colunas de acordo com os grupos para os quais a empresa tenha ofertado a melhor proposta, com o detalhamento do objeto a ser fornecido, observadas as especificações contidas no Termo de Referência.

ANEXO I-III - LISTA DE VERIFICAÇÃO (TERMO DE RECEBIMENTO DEFINITIVO)

TERMO DE RECEBIMENTO DEFINITIVO - BENS				
Processo SEI Relacionado: **Edital de Licitação TSE nº (se for o caso):** **Contratada:** **CNPJ nº:** **Contrato/Nota de Empenho:** **Objeto:** **Prazo de Entrega:**				
Fiscalização: Memorando nº (SEI nº) **Fiscal Técnico Titular:** **Fiscal Técnico Substituto:**				
ITEM	**CRITÉRIO DE CONFERÊNCIA**	**SIM**	**NÃO**	**N.A.**
1	**ASPECTOS QUANTITATIVOS DA AQUISIÇÃO:**			
1.1	A quantidade entregue corresponde à totalidade do previsto no empenho/contrato?			
1.2	Os materiais foram entregues dentro do prazo previsto?			
1.3	O quantitativo de acessórios (cabos, conectores) é compatível com o número de equipamentos adquiridos			
1.4	No caso de reprovação dos materiais entregues, estes foram substituídos nos prazos previstos?			
2	**ASPECTOS QUALITATIVOS DA AQUISIÇÃO**:			
2.1	A marca dos materiais entregues correspondem ao previsto na proposta da empresa?			
2.2	Todos os itens possuem especificações compatíveis com o Edital e correspondentes à proposta da licitante vencedora? Os materiais entregues estão em conformidade com as especificações do Termo de Referência?			
2.3	Todos os equipamentos possuem indicação de garantia do fabricante?			
2.4	Todos os equipamentos estão funcionando?			
2.5	A instalação da solução foi realizada com sucesso?			
3	**OUTRAS OBRIGAÇÕES CONTRATUAIS**:			
3.1	O valor dos produtos descrito na nota fiscal corresponde ao previsto na contratação?			
3.2	O CNPJ constante da nota fiscal corresponde ao expresso no empenho?			
	HOUVE ABERTURA DE PROCESSO ADMINISTRATIVO PARA APLICAÇÃO DE PENALIDADES? **SEI nº:**			
RELATÓRIO DE OCORRÊNCIAS				
RECEBIMENTO DEFINITIVO DO OBJETO				
Efetuada a análise de conformidade do objeto com as especificações do Termo de Referência e do instrumento contratual, quanto aos aspectos quantitativos, qualitativos e de obrigações contratuais, a fiscalização decide, ressalvadas eventuais observações contidas no Relatório de Ocorrências, por:				
	RECEBER DEFINITIVAMENTE O OBJETO			
	NÃO RECEBER DEFINITIVAMENTE O OBJETO			

TERMO DE RECEBIMENTO DEFINITIVO - SERVIÇOS				
Processo SEI Relacionado: **Edital de Licitação TSE nº (se for o caso):** **Contratada:** **CNPJ nº:** **Contrato/Nota de Empenho:** **Objeto:** **Prazo de Entrega:**				
Fiscalização: Memorando nº (SEI nº) **Fiscal Técnico Titular:** **Fiscal Técnico Substituto:**				
ITEM	**CRITÉRIO DE CONFERÊNCIA**	**SIM**	**NÃO**	**N.A.**
1	**ASPECTOS QUANTITATIVOS DO SERVIÇO:**			
1.1	O serviço foi prestado no quantitativo de horas previsto no contrato?			
1.2	Os produtos obrigatórios foram entregues?			
1.3	Houve entregas parciais? (se sim, relatar no relatório de ocorrências deste Termo)			
1.4	No caso de reprovação de serviços entregues, estes foram ajustados nos prazos previstos?			
2	**ASPECTOS QUALITATIVOS DO SERVIÇO:**			
2.1	Os serviços atenderam aos critérios definidos na ordem de serviço?			
2.2	Os serviços foram executados conforme as especificações deste Termo de Referência?			
2.3	Houve acionamento de serviços em caráter emergencial?			
2.4	Todos os equipamentos que dependam dos serviços prestados estão funcionando?			
	HOUVE ABERTURA DE PROCESSO ADMINISTRATIVO PARA APLICAÇÃO DE PENALIDADES? **SEI nº:**			
RELATÓRIO DE OCORRÊNCIAS				
RECEBIMENTO DEFINITIVO DO OBJETO				
Efetuada a análise de conformidade do objeto com as especificações do Termo de Referência e do instrumento contratual, quanto aos aspectos quantitativos, qualitativos e de obrigações contratuais, a fiscalização decide, ressalvadas eventuais observações contidas no Relatório de Ocorrências, por:				
	RECEBER DEFINITIVAMENTE O OBJETO			
	NÃO RECEBER DEFINITIVAMENTE O OBJETO			

ANEXO I-IV - DESIGNAÇÃO DE PREPOSTO

DESIGNAÇÃO DE PREPOSTO
A empresa **Nome da Empresa**, com sede na **Endereço da empresa**, na cidade de **Cidade**, (**UF**), CNPJ nº **000.000.000/0000-0**, neste ato representada pelo seu **Cargo do Representante**, Senhor(a) **Nome do Representante** portador(a) da Carteira de Identidade nº **Identidade do Representante**, CPF nº **CPF do Representante**, em atenção ao art. 44 da IN MPDG nº 5/2017, DESIGNA, o(a) Senhor(a) **Nome do Colaborador**, portador(a) da Carteira de Identidade nº **Identidade do Colaborado**, CPF nº **CPF do Colaborador**, para atuar como preposto no âmbito do **Contrato TSE nº xx/xxxx**.
2. O preposto designado representará a empresa perante o Tribunal Superior Eleitoral, zelará pela boa execução do objeto contratual, exercendo os seguintes poderes e deveres:
a) Ser acessível ao Contratante, por intermédio do email e dos números de telefone fixo e celular informados neste formulário.
b) Acatar as recomendações efetuadas pelo fiscal do contrato.
c) Participar de reunião inaugural a ser agendada com a fiscalização do contrato;
d) Desenvolver outras atividades de responsabilidade da Contratada, principalmente quanto ao controle de informações relativas ao seu contrato, emissão de relatórios e apresentação de documentos quando solicitado.
3. A comunicação entre o preposto e o Tribunal Superior Eleitoral será efetuada por meio dos telefones fixo **(DDD) 00000-0000** e celular **(DDD) 00000-0000**ou do e-mail **email@email.com.br**. 4. A **Nome da Empresa** compromete-se a manter atualizados, durante toda fase de execução da contratação, os contatos de telefone e e-mail para comunicação com o Tribunal Superior Eleitoral.

ANEXO I-V – TERMO DE VISTORIA

Declaramos, para fins de participação no Pregão TSE nº _____, que a empresa _____, devidamente representada pelo Sr. _____, CPF nº _____, realizou vistoria técnica junto a este Tribunal Superior Eleitoral, tomando conhecimento sobre os locais do TSE onde deverão ser instalados/configurados os equipamentos, verificando localização no Data Center onde serão instalados os novos equipamentos, os modelos de equipamentos utilizados pelo TSE, inclusive switches em que serão conectados; tendo sanado quaisquer possíveis dúvidas sobre as especificações constantes do Edital.

Brasília, _____ de _____ de 2023.

_____
Representante da licitante

_____
Representante do TSE

ANEXO I- VI - TERMO DE CONFIDENCIALIDADE PARA VISTORIA TÉCNICA

Eu <nome, nacionalidade, estado civil, cargo> inscrito(a) no CPF sob o nº XXX.XXX.XXX-XX, assumo o compromisso de manter a confidencialidade sobre todas as informações obtidas em função da participação em certame licitatório junto a CONTRATANTE. Por este termo de confidencialidade e sigilo comprometo-me:

1. A não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e / ou unilateral, presente ou futuro, ou para o uso de terceiros.

2. A não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso.

3. A não apropriar-se para si ou para outrem de material confidencial e / ou sigiloso da tecnologia que venha a ser disponível.

4. A não repassar o conhecimento das informações confidenciais, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e / ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

Neste Termo, as seguintes expressões serão assim definidas:

Informação Confidencial significará toda informação revelada através da apresentação da tecnologia, a respeito de, ou, associada com a Avaliação, sob a forma escrita, verbal ou por quaisquer outros meios.

Informação Confidencial inclui, mas não se limita, à informação relativa às operações, processos, planos ou intenções, informações sobre produção, instalações, equipamentos, sistemas, dados, habilidades especializadas, projetos, métodos e metodologia, fluxogramas, especializações, componentes, fórmulas, produtos e questões relativas ao desempenho das atividades laborais.

Avaliação significará todas e quaisquer discussões, conversações ou negociações entre, ou com as partes, de alguma forma relacionada ou associada com a apresentação da tecnologia, projetos ou produtos.

A vigência da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste termo, terá a validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo.

Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

Brasília, _____ de _____ de 2023.

_____
Representante da licitante

ANEXO I- VII - MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO (OS)			
N° da Ordem de Serviço	**Data de Emissão da OS**	**N° do Contrato**	**Data de Assinatura do Contrato**
Área Requisitante		**Requisitante Responsável**	

IDENTIFICAÇÃO DA EMPRESA CONTRATADA		
Nome da Empresa		
CNPJ		**Inscrição Estadual**
Endereço		
Cidade	**Estado**	**CEP**
Telefone	**E-mail institucional**	
Preposto		

OBJETO DO CONTRATO:

ESPECIFICAÇÃO DOS SERVIÇOS A SEREM EXECUTADOS

Item	Descrição	Horas consumidas	Valor total (R$)
01			
02			
03			
04			
		Valor total da OS:	

DETALHAMENTO DOS SERVIÇOS A SEREM EXECUTADOS E DAS ENTREGAS

PERÍODO DE EXECUÇÃO DOS SERVIÇOS

Data de Início da Execução: ____/____/_____	**Data de Término da Execução: ____/____/_____**

APROVAÇÃO DO GESTOR DO CONTRATO

Solicitação:

Solicitamos a realização do serviço acima caracterizado, nos termos constantes desta Ordem de Serviços, que tem por base as obrigações e responsabilidades da contratada constantes do contrato firmado, supra indicado.

<Nome do Fiscal Requisitante>

Matrícula

Fiscal Requisitante

Autorização

Autorizo a realização do serviço acima caracterizado, nos termos constantes desta Ordem de Serviços, que tem por base as obrigações e responsabilidades da contratada constantes do contrato firmado, supra indicado.

<Nome do Gestor do Contrato >

Matrícula

Gestor do Contrato

CIENTE DA CONTRATADA

Declaramos nossa ciência e concordância com as condições registradas nesta Ordem de Serviços para execução dos serviços solicitados.

<Nome do Representante Legal da Contratada>

CPF:

Preposto da Contratada

Obs: o modelo poderá ser ajustado visando melhor adequar-se à necessidade de serviço

ADAÍRES AGUIAR LIMA
SECRETÁRIA DE ADMINISTRAÇÃO

Documento assinado eletronicamente em **01/12/2023, às 14:47**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

Tribunal Superior Eleitoral

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=2697900&crc=734676EA, informando, caso não preenchido, o código verificador **2697900** e o código CRC **734676EA**.