ESTUDOS TÉCNICOS / 2023 - SEINF

1. IDENTIFICAÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

SOLUÇÃO DE TI	
NOME DA SOLUÇÃO DE TI:	*Secure Web Gateway* (SWG)
ÁREA DEMANDANTE:	Coordenadoria de Desenvolvimento e Infraestrutura
E-MAIL DO DEMANDANTE:	rosemberg.maia@tre-pi.jus.br
TELEFONE DO DEMANDANTE:	86 2107-9762

2. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

A solução consiste no fornecimento, instalação e configuração de sistema de filtragem e otimização de conteúdo web via provimento de funcionalidades de "Secure Web Gateway" (SWG), incluindo testes operacionais, operação assistida e demais componentes necessários ao seu perfeito funcionamento, bem como os serviços de migração, treinamento, garantia, consultoria e suporte técnico.

A solução de *Secure Web Gateway* (SWG) visa a mitigação do risco de ataques cibernéticos e bloqueio de acesso dos usuários a sites e aplicativos maliciosos.

O *Secure Web Gateway* (SWG) é um produto de segurança cibernética que protege os dados da instituição e aplica políticas de segurança. Os SWG's filtram o conteúdo inseguro do tráfego web para deter as ameaças cibernéticas e as invasões de dados. Eles também bloqueiam comportamentos arriscados ou não autorizados do usuário.

Um SWG e um firewall são similares porque ambos fornecem proteção avançada de redes e estão aptos a identificar tráfego malicioso. Contudo, um firewall funciona com análises ao nível de pacote de dados, enquanto um SWG atua com análises de tráfego no nível da aplicação em si.

3. MOTIVAÇÃO / JUSTIFICATIVA

Os serviços *web* baseados na rede mundial de computadores são imprescindíveis e valiosos para toda a organização, e tornaram-se um facilitador para a comunicação entre os seus usuários e o acesso a uma ampla gama de informações precípuas. Entretanto, o acesso à Internet contém sério risco à segurança e à produtividade.

Nesse âmbito, existem estimativas indicando que cerca de 40% de todo o tráfego da Internet corporativa não está relacionado ao negócio, o que pode acarretar na minimização de produtividade dos funcionários, bem como no consumo de recursos da rede para propósitos não vinculados aos processos de negócio da organização.

Diante dessa situação, e uma vez que exista um mecanismo automatizado para fins de categorização das diversas páginas da Internet por assunto, torna-se possível o bloqueio ou a liberação de todos os sites relacionados à categoria escolhida. Assim, é possível o controle dos acessos aos sites da Internet, facilitando o controle gerencial dos acessos, visto que tal mecanismo permite a emissão de relatórios detalhados de como e por quem os sites estão sendo visitados, mantendo-se um histórico de todos os acessos em um repositório de dados centralizado.

Tais requisitos técnicos e de negócio são satisfatoriamente atendidos por meio de um sistema especializado em tais atividades, geralmente denominado pela literatura especializada de sistema de controle e gerenciamento de conteúdo "web". Um sistema de controle e gerenciamento de conteúdo "web" ("Secure Web Gateway" - SWG) consiste em um conjunto de componentes de "hardware" e/ou "software" implementados em sistemas operacionais convencionais por meio da instalação de "software" em sistemas dedicados do tipo "appliance" físicos e/ou virtuais hospedados em ambiente local do "datacenter" ou em ambiente de nuvem computacional (pública ou híbrida).

Em relação ao funcionamento, alguns SWG´s são executados em servidores proxy, que, por sua vez, são dispositivos conctados à rede que fazem solicitações e recebem respostas em nome de um dispositivo cliente (por exemplo, uma estação de trabalho, laptop ou smarphone do usuário) ou de outro servidor. Para os SWG´s, esse servidor proxy pode ser um servidor físico real ou uma máquina virtual na nuvem. Outros SWGs são apenas softwares, que podem ser executados nas instalações de uma empresa ou na nuvem como um aplicativo SaaS. E, finalmente, alguns SWGs são implantados como aparelhos locais: dispositivos físicos de hardware que se conectam à infraestrutura de TI de uma empresa.

Um sistema SWG usualmente atua como "Web Proxy" das estações de trabalho dos usuários de uma dada rede IP interna, filtrando todo o tráfego "web" de navegação na Internet de uma organização e permitindo que o administrador da rede implemente políticas de acesso mais efetivas, frequentemente por meio do emprego de uma base de dados com milhares de URLs e aplicativos reconhecidos pelo sistema, de tal maneira que permite o administrador de rede definir e implementar políticas de acesso à rede mundial de computadores mais assertivas e com baixo custo de gerenciamento, além de atender a demandas forenses e legais tais como o Marco Civil da Internet brasileira e a Lei Geral de Proteção de Dados, por exemplo.

Importante frisar, com base nas diretrizes definidas na Estratégia Nacional de Cibersegurança, definidas pelo Tribunal Superior Eleitoral (TSE), que vários investimentos em Tecnologia da Informação e Comunicação (TIC) estão sendo realizados para modernizar sua infraestrutura de TIC com a finalidade mitigar o risco de ataques cibernéticos.

Dessa forma, visando ao alinhamento estratégico e ganho em escalabilidade, disponibilidade e confiabilidade na entrega dos serviços

prestados à sociedade, o TRE-PI pretende adquirir solução de *Secure Web Gateway* (SWG) que compreende funções de filtro de conteúdos, controle de aplicações, prevenção de perda de dados (*Data Loss Prevention* - DLP), software antimalware e inspeção HTTPS.

Diante disso, propõe-se a aquisição de Solução de Secure Web Gateway (SWG), visando à segurança e ao bom desempenho das atividades no âmbito desta Justiça Especializada.

Conforme exposto, a aquisição fundamenta-se em razão da necessidade de mitigar os inúmeros riscos a que estão expostos os usuários do Tribunal e, consequentemente, aumentar a confiabilidade, integridade e a disponibilidade dos serviços oferecidos ao público interno e à sociedade, segundo as melhores práticas do mercado de segurança da informação.

A motivação da contratação se dá, portanto, com base nas seguintes necessidades:

- No quesito segurança, pelo oferecimento de uma camada adicional de defesa, protegendo os usuários dos serviços, e executando funções de segurança de proteção através da aplicação de regras de segurança da organização;
- Ainda no quesito segurança, pela filtragem de URL em tempo real para identificar sites potencialmente maliciosos que possam comprometer a organização;
- No quesito desempenho, pela melhoria de acesso aos conteúdos dinâmicos;
- No quesito *compliance*, garantida adequação à LGPD através da proteção dos dados e informações da organização;
- Ampliar o controle de perímetro, por meio da inspeção e análise contínuo de tráfego das aplicações;
- Aprimorar os mecanismos de monitoramento e detecção de ataques;
- Proporcionar a prevenção e mitigação de ameaças cibernéticas;
- Contribuir para a redução da superfície de ataques cibernéticos da Justiça Eleitoral.

4. RESULTADOS ESPERADOS

- Aumento da resiliência a ciberataques nos serviços de TI.
- Aumentar o nível de eficiência de uso dos canais de comunicação.
- Aumentar o grau de proteção contra códigos maliciosos (ou malware).
- Aumentar o nível de produtividade dos recursos humanos empregados pelo Poder Judiciário.
- Reduzir os custos com canais de comunicação de dados.

5. REQUISITOS DE NEGÓCIO

5.1 – Requisitos funcionais (Necessidades de negócio)

NECESSIDADE 1			
Filtragem de URLs e de reputação "online" do conteúdo "web".			
ID	**FUNCIONALIDADE**	**RESPONSÁVEL**	**ÁREA**
1	Categorização de "web sites" conhecidos em grupos permitindo o bloqueio.	Área demandante	CODIN
2	Obtenção de relatórios de uso com maior grau de detalhe e de especificidade da demanda.	Área demandante	CODIN

NECESSIDADE 2			
Filtragem de "malwares".			
ID	**FUNCIONALIDADE**	**RESPONSÁVEL**	**ÁREA**
1	Proteção contra softwares potencialmente maliciosos ("malwares").	Área demandante	CODIN
2	Proteção contra softwares não autorizados.	Área demandante	CODIN

NECESSIDADE 3			
Controles ao nível das aplicações "web".			
ID	**FUNCIONALIDADE**	**RESPONSÁVEL**	**ÁREA**
1	Gerenciamento de aplicações baseadas na Internet (mensageria instantânea, telefonia via Internet, redes ponto-a-ponto, videoconferências, redes sociais, etc) com maior grau de especificidade por usuário.	Área demandante	CODIN

5.2 – Requisitos não-funcionais

ID	**TIPO**	**REQUISITO**

1	Requisitos de capacitação	Trata-se do serviço de treinamento da solução, na modalidade de fornecimento de voucher para treinamento, cujo escopo cubra conceitos de configuração, operação, administração, gerência, otimização, resolução de problemas e gestão de todos os componentes da solução de forma que os participantes capacitados possam colocar a solução em produção, bem como planejar mudanças de configuração no ambiente. 1. O treinamento deverá oferecer carga horária total de no mínimo 20 (vinte) horas. 2. Serão aceitos apenas treinamentos nas modalidades online ao vivo (EAD), podendo as aulas serem gravadas, a critério da CONTRATANTE. 3. A CONTRATADA deverá prover capacitação técnica em turma com no mínimo 1 (um) e no máximo 8 (oito) participantes. 4. O treinamento deverá respeitar o limite de 4 (quatro) horas por dia. 5. O treinamento deverá cobrir conhecimentos necessários para instalação, administração, configuração, gerência, otimização, resolução de problemas e utilização da solução. As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA. O treinamento poderá ser composto de mais de 01 (um) módulo, que deverão ser discriminados na proposta da licitante. A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar que o(s) treinamento(s) ofertado(s) atende(m) os requisitos indicados nos itens anteriores. O Tribunal poderá planejar e escolher qualquer das datas, ou períodos, dos eventos de capacitação no prazo de validade da ata de registro de preços, a contar da entrega do calendário. O treinamento deverá ser ministrado em data oportuna a ser informada à fiscalização após ou antes da instalação da solução, ficando a critério da administração e baseando-se no calendário a ser fornecido pela CONTRATADA. É permitido à CONTRATADA terceirizar o treinamento a outra que preste serviços de treinamento da solução ofertada, ou ao próprio fabricante, desde que mantidas as demais condições deste documento e permanecendo ela a única responsável pelo atendimento do contratado para todos os fins. O treinamento deverá ser ministrado por profissionais certificados pelo fabricante (com a certificação mais alta do fabricante), cuja comprovação deverá ser encaminhada na assinatura do Contrato. A CONTRATADA deverá fornecer material didático individual, na modalidade digital, que abranja todo o conteúdo do(s) curso(s). Todo o material didático oferecido pela CONTRATADA para realização do treinamento deverá estar atualizado e poderá estar em inglês ou português. O treinamento deverá ser ministrado em português do Brasil. Caso não exista material oficial do produto em língua portuguesa, será aceito material em inglês. O treinamento deverá oferecer acesso a laboratório prático virtual, fornecido pela CONTRATADA, para configuração e execução de exercícios práticos. • No ambiente de treinamento, os servidores indicados pelo CONTRATANTE deverão ter acesso em ambiente de laboratório a todos os produtos ofertados (ou similares) para realização da capacitação. A CONTRATADA deverá emitir para o servidor participante, sem ônus para o Tribunal e no prazo máximo de até 10 (dez) dias úteis após o término do treinamento, o certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia deste certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento. A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo a CONTRATADA informar no certificado a carga horária e assiduidade do servidor.

2	Requisitos Legais	A CONTRATADA deverá observar o cumprimento de todas as leis e normas aplicáveis ao OBJETO, em especial atenção àquelas relacionadas ao pagamento das obrigações empresariais relacionadas à encargos fiscais, trabalhistas e previdenciários. Outras Referências: • Resolução TRE-PI nº 458/2022, que dispõe sobre a Política de nivelamento, atualização e renovação da infraestrutura de Tecnologia da Informação no âmbito da Justiça Eleitoral do Piauí; • Resolução CNJ n° 182/2013, dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ); • Resolução CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD); • Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ); • LGPD – Lei Geral de Proteção de Dados (Lei n° 13.709/2018) e Marco Civil da Internet Lei no 12.965/2014); • Resolução TSE Nº 23.644, de 1º de julho de 2021, Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral; • Lei nº 8.666/1993, regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências; • Lei nº 14.133, de 1º de abril de 2021, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios; • Instrução Normativa Nº 1, de 4 de abril de 2019. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal; • Decreto nº 9.488/2018, altera o Decreto nº 7.892, de 23 de janeiro de 2013, que regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993, e o Decreto nº 7.579, de 11 de outubro de 2011, que dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal.
		A CONTRATADA deverá fornecer garantia técnica de pelo menos 36 (trinta e seis) meses para a solução, contados a partir da data de emissão do Termo de Recebimento Definitivo relativo à fase de instalação; Os serviços de garantia técnica englobam todos os elementos de hardware e software da solução, incluindo a prestação de serviços de suporte técnico, assistência corretiva e atualização tecnológica, compreendendo a substituição de peças, componentes, acessórios e aplicativos que apresentem defeito, ou precisem ser atualizados durante este período, sem qualquer ônus adicional para o CONTRATANTE, obrigando-se a CONTRATADA a manter os appliances e aplicativos permanentemente em perfeitas condições de funcionamento para a finalidade a que se destinam; A garantia técnica compreenderá todas as funcionalidades da solução ofertada, tanto as descritas no Termo de Referência quanto as contempladas nos manuais e demais documentos técnicos, incluindo a atualização de versões de software; Qualquer software ou equipamento com hardware defeituoso, peças quebradas, com defeito ou gastas pelo uso normal deverá ser substituído por outro de mesma marca e modelo e com as mesmas características técnicas ou superiores, novo e de primeiro uso, no prazo de 07 (sete) dias úteis a partir de notificação do CONTRATANTE; A CONTRATADA deverá apresentar no protocolo do CONTRATANTE, antes do início da vigência do serviço de garantia técnica, todos os dados necessários para o registro de chamados técnicos na Central de Atendimento da CONTRATADA, tais como, e-mail, números de telefone e fax, etc; Suporte Técnico durante o período de Garantia Técnica: • Durante o período de garantia técnica de 36 (trinta e seis) meses, a partir do recebimento definitivo da instalação, a CONTRATADA deverá garantir o funcionamento de toda a solução, fornecer atualizações, prestar suporte técnico e atender aos chamados técnicos para manutenção; • A CONTRATADA deverá comunicar formalmente ao Gestor do Contrato a disponibilidade de novas versões e releases das licenças de software e firmwares, reservando-se, à equipe técnica do CONTRATANTE, o direito de exigir a atualização sem que isso implique acréscimo aos preços contratados; • A manutenção corretiva será realizada em período integral, 7 (sete) dias por semana e 24 (vinte e quatro) horas por dia, após solicitação do CONTRATANTE; A CONTRATADA deverá entregar no protocolo do CONTRATANTE, mensalmente, até o

3	Requisitos de Manutenção	5° (quinto) dia útil do mês subsequente, para fins de controle, Relatório Gerencial dos Serviços (RGS) realizado no mês anterior. Deverão constar, no mínimo, as seguintes informações: • Relação de todos os chamados técnicos ocorridos no mês anterior, incluindo data e hora do início e término do suporte; identificação do problema; criticidades; providências adotadas para o diagnóstico, solução provisória e solução definitiva; data e hora do início e término da solução definitiva; identificação do técnico do CONTRATANTE que solicitou e validou o chamado; identificação do técnico da CONTRATADA responsável pela execução do chamado, bem como outras informações pertinentes; • Cada chamado técnico aberto será avaliado individualmente pelo Gestor do Contrato; • O serviço será considerado recebido pelo Gestor do Contrato quando do fechamento de cada chamado, desde que não reapareçam posteriormente ao fechamento inconformidades técnicas comprovadamente relacionadas ao chamado recebido; • O Gestor do Contrato emitirá a recusa em caso de verificação de impropriedades ou erros impeditivos de recebimento do serviço prestado. A CONTRATADA deverá promover as correções necessárias, conforme diretrizes a serem estabelecidas pelo Gestor do Contrato, sem prejuízo de aplicação de penalidades previstas. A CONTRATADA deverá fornecer versão atualizada do manual e demais documentos técnicos sempre que houver atualização nos manuais, nos softwares ou nos appliances da solução; A CONTRATANTE poderá realizar a aplicação de pacotes de correção e migração de versões e releases das licenças de software, quando lhe for conveniente, cabendo à CONTRATADA orientar e colocar à disposição um técnico para contato em caso de dúvidas ou falhas. A CONTRATANTE reserva-se o direito de proceder a outras configurações, instalações ou conexões nos appliances, desde que tal iniciativa não implique em danos físicos e lógicos aos appliances, sem que isto possa ser usado como pretexto pela CONTRATADA para se desobrigar do suporte da solução; A CONTRATADA deverá garantir pleno funcionamento dos appliances e softwares, bem como atualizações, responsabilizando-se por qualquer componente adicional que for identificado após a contratação, seja por motivos de interoperabilidade, compatibilidade ou quaisquer outros motivos que impeçam o funcionamento efetivo da solução CONTRATADA; A CONTRATADA deverá dispor de serviço de esclarecimento de dúvidas relativas à utilização dos appliances e de abertura de chamado técnico por e-mail ou por telefone 0800 (gratuito), ou telefone local por todo o período da garantia técnica; A CONTRATADA deverá garantir, sem quaisquer custos adicionais, as atualizações havidas nos appliances nas versões de software e firmware, inclusive releases, pelo prazo de vigência da garantia; O serviço de garantia técnica deverá permitir o acesso do CONTRATANTE à base de dados de conhecimento do fabricante dos appliances, provendo informações, assistência e orientação para diagnósticos, avaliações e resolução de problemas, características dos produtos e demais atividades relacionadas à correta operação e funcionamento dos mesmos; As atualizações e correções (patches) do software e firmwares deverão estar disponibilizados via WEB ou fornecidas em mídia (CD ou DVD), quando desta forma forem solicitadas; Quando a garantia técnica for acionada, o atendimento deverá ser iniciado imediatamente, independente do meio utilizado. A cada abertura de chamado, a CONTRATADA deverá fornecer ao CONTRATANTE um código identificador único para acompanhamento; A CONTRATADA deverá conceder acesso ao CONTRATANTE ao controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do Gestor do Contrato.

4	Requisito Temporal	Deverá ser realizada, após a assinatura do Contrato, uma reunião de alinhamento remota, com o objetivo de alinhar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e em seus Anexos, e esclarecer possíveis dúvidas acerca do objeto, conforme agendamento efetuado pelo Gestor do Contrato, bem como: • Apresentar a relação do pessoal técnico especializado, adequado e disponível para a execução do objeto deste Estudo, bem como a qualificação de cada um dos membros da equipe técnica. • Apresentar a declaração de disponibilidade, assinada por cada integrante da equipe técnica mencionada na alínea anterior, bem como o Termo de Confidencialidade da Informação. • Apresentar um cronograma para implantação e configuração da Solução adquirida, o qual deverá sofrer aval do Gestor do Contrato. • Apresentar a logística para realização do treinamento da Solução adquirida. • Os profissionais indicados pela CONTRATADA deverão efetivamente implantar e configurar a Solução objeto deste Estudo, admitindo-se suas substituições por profissionais de experiência equivalente ou superior, desde que aprovada previamente pelo órgão. • O prazo para a entrega da solução será de até 90 (noventa) dias consecutivos, contados a partir do primeiro dia útil após a confirmação de recebimento da Ordem de Fornecimento emitida pela Fiscalização do Contrato. • O prazo de implantação da solução será de até 30 (trinta) dias consecutivos a partir do recebimento do objeto.
5	Requisitos de Segurança da Informação	A CONTRATADA deverá submeter-se aos procedimentos de segurança existentes, ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessária a presença nas dependências da CONTRATANTE. A empresa CONTRATADA deverá respeitar as diretrizes constantes da Política de Segurança da Informação do da Justiça Eleitoral (Resolução TSE No 23.501/2016), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Piauí, e de outros partícipes desta contratação, aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa; O Tribunal Regional Eleitoral do Piauí terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação; Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX). O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e a proteger todos os dados de infraestrutura e de vulnerabilidades do CONTRATANTE a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.
6	Requisitos Sociais, Ambientais e Culturais	A documentação e os manuais da solução deverão, preferencialmente, ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês. Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil). O licenciamento e o suporte deverão ser prestados preferencialmente no idioma português do Brasil. Os softwares aplicativos e interface do software deverão ter a possibilidade de escolha de idioma pelo usuário. Será admitido o idioma inglês somente quando não existir uma versão no idioma português do Brasil. Os profissionais da CONTRATADA deverão trajar-se de maneira respeitável e usar linguagem respeitosa e formal no trato com os servidores do órgão, Gestão Contratual e os dirigentes da CONTRATANTE.
7	Requisitos de Desempenho	Não se aplica

5.3 – Requisitos tecnológicos

ID	TIPO	REQUISITO
		1. DESEMPENHO, CAPACIDADE E ALTA DISPONIBILIDADE: a. A solução de Secure Web Gateway deverá ser de arquitetura dedicada para este fim, isto é, do tipo "appliance" físico ou virtual, instalado e configurado para fazer o tratamento do tráfego de dados dentro da infraestrutura pertencente a este Tribunal Regional Eleitoral do Píauí, não podendo ser servidor de uso genérico;

b. Não serão aceitos soluções do tipo SaaS ("Software as a Service") que façam o envio e tratamento no tráfigo de dados fora da infraestrutura pertencente a este Tribunal Regional Eleitoral do Piauí.

c. Caso a solução oferecida seja do tipo "aplliance virtual", deverá ser totalmente compatível com infraestrutura computacional hiperconvergente baseada em tecnologia VMWare.

d. Caso a solução oferecida seja do tipo "aplliance físico", deverá ser fornecido com:

1. No mínimo 03 (três) interfaces 10/100/1000BaseT, sendo uma destas dedicada ao gerenciamento da solução;

2. Fonte de alimentação elétrica redundante e hot swappable, com chaveamento automático e capacidade de operar nas tensões de 100 a 240 V, 50 – 60Hz. A fonte fornecida deverá suportar sozinha a operação da unidade com todos os módulos de interface ativos. Não serão aceitas fontes redundantes externas ao equipamento;

3. Cabos elétricos com conector padrão 2P+T, e quaisquer acessórios necessários para interligação do equipamento à rede elétrica do TRE-PI. A necessidade de qualquer mudança nas tomadas (plugs) para adequação à rede elétrica será de responsabilidade da CONTRATADA, a qual deverá assegurar a manutenção e garantia dos appliances fornecidos;

4. Unidade de armazenamento de, no mínimo, 100GB;

5. Suporte a montagem em Rack de 19";

e. A solução deverá prover as funcionalidades de Proxy HTTP/HTTPS, Filtro de Conteúdo, Caching e AntiMalware, incluindo e inspeção de tráfego SSL e Monitoramento de camada quatro do modelo OSI;

f. Todas as funcionalidades especificadas dos appliances deverão estar aptas e licenciadas no ato de sua aquisição, sem custos adicionais para sua plena utilização; caso ocorra a necessidade de instalação de Patch's e atualização de Firmware os mesmos não poderão afetar as funcionalidades exigidas neste edital;

g. Deverá prover o serviço para no mínimo 700 usuários simultâneos;

h. Deverá ser licenciado para suportar a quantidade de 1.500 de usuários totais;

i. Deverá prover armazenamento temporário de objetos (cache) e ainda permitir que seja definido o tamanho máximo de objetos;

j. O equipamento oferecido deverá permitir o adicionamento de licenças para até 1.500 usuários sem a necessidade de upgrades físicos;

l. Deverá ser composta por dois appliances em cluster Ativo-Ativo e Ativo-Passivo com processamento e alimentação individual, de maneira que, caso ocorra uma parada ou defeito parcial de um dos appliances, isso não interfira de modo algum no funcionamento da solução, sendo um dos nós capaz de suportar a capacidade total exigida para a solução, bem como licenciamento;

m. Caso o appliance físico não execute a função de gerenciamento unificado e emissão de relatórios, será admitido o gerenciamento unificado através de appliance virtual compatível com o ambiente virtualizado do TRE-PI, a saber: VSphere 7.0 ou superior;

n. A solução deverá permitir a configuração manual e automática de horário através de uso NTP ou SNTP;

o. Deverá possuir suporte a implementação e compatibilidade com os protocolos IPv4 e IPv6;

p. HA (Alta disponibilidade) em appliances distintos de forma a permitir alta disponibilidade de site. Por alta disponibilidade entende-se que um único appliance deverá ser capaz de sustentar a todos os requisitos da presente documentação sem perda de performance.

2. GERENCIAMENTO:

a. Deverá possuir capacidade de integração com Serviços de Domínio Active Directory Windows (AD DS), possibilitando o gerenciamento e administração da ferramenta com base nas informações deste serviço;

b. A autenticação deverá ser baseada em ao menos dois dos quatro seguintes protocolos: NTLM, kerberos, ldap, radius. A autenticação deverá ocorrer de modo transparente, ou seja, utilizando usuário já autenticado em domínio Windows sem pedir novamente a senha de acesso (Single Sign-On);

1	Requisitos da Arquitetura Tecnológica	c. A autenticação de usuários e estações de trabalho deverá ocorrer sem a necessidade de instalação ou execução de clientes ou quaisquer módulos em nenhuma estação de trabalho ou servidor; d. A capacidade para gerência e administração da ferramenta deverá possibilitar a concessão de direitos a usuários e grupos com no mínimo três níveis de privilégios, como por exemplo: Administrador, operação e emissor de relatórios; e. Todas as operações da solução deverão ser executadas em console único, e somente será admitida a necessidade de acesso a outros consoles para tarefas de manutenção da ferramenta e troubleshooting (resolução de problemas); f. Deverá possuir gerenciamento gráfico (web) do equipamento via protocolo HTTP ou HTTPS de forma intuitiva e amigável (point-and-click), possibilitando todo gerenciamento, tais como criação de políticas, resolução de problema e acesso a relatórios, sem a necessidade da CLI (Command Line Interface) ou semelhante, como, por exemplo, CLI HTTP; g. Deverá possuir auditoria de configuração, gravando e disponibilizando todas as alterações que identifique, no mínimo, quem, quando e o que foi alterado; h. Deverá permitir a execução de cópias de segurança (backup) de forma manual e automática, e permitir também a restauração destas cópias; i. Deverá implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps. **3. CONTROLE DE APLICAÇÕES:** a. Deverá permitir a criação de regras que possibilite a permissão ou bloqueio de aplicações diversas tais como: • Entretenimento: IM, proxy anônimo e similares; • Acesso remoto: Logme-in, Team Viewer, VNC e similares; • Potenciais consumidores de banda: P2P, Média Players e similares; b. Suportar os protocolos HTTP, HTTPS e FTP, em seus modos ativo e passivo. **4. FILTRO DE ACESSO:** a. Deverá permitir a criação de regras que possibilite a permissão ou bloqueio de acesso baseado nos seguintes critérios: • Origem (Grupos do domínio ou serviço de diretórios LDAP e AD ao qual o usuário pertence; Aplicação); • Destino (Categoria, domínio, url/lista); • Tipo de arquivo; • Protocolos (HTTPS, FTP e outros); • Horário (definir períodos de funcionamento por regra); b. Deverá permitir definição de largura ou porcentagem de banda máxima para o acesso de acordo com o estabelecido em regra, baseando-se em categoria do destino ou protocolo; c. A solução deve atuar como “man in the middle”, intermediando e repassando todas as requisições. Deverá suportar certificados on-box, importando certificados validos ou gerando auto-assinados. Deverá permitir a emissão de páginas amigáveis e customizáveis de erro também aos sites criptografados; d. Deverá permitir o controle de acesso através do percentual de largura de banda disponível para determinadas Categorias e os limites de banda deverão ser definidos por: • Limite de Banda ou percentual de Banda - Definindo um limite global para todos os usuários da rede para os tipos de aplicativos para definir um limite global de largura de banda para restringir a quantidade de tráfego de rede; • Limite de Banda por Usuário. Definindo um limite individual para cada usuário da rede para os tipos de aplicativos para definir um limite de largura de banda para restringir a quantidade de tráfego de rede; e. Deverá permitir a definição de quota de acesso, tornando possível que determinados destinos (Categorias/URL/Domínio/Lista) possam ser acessados por um período limitado de tempo, e que possa ser consumido de modo não contínuo. Para exemplificação prática, espera-se como resultado que cada usuário do grupo especificado poderá acessar o conteúdo definido na quota, em qualquer momento do dia, porém a soma de tempo deste consumo, não deverá ultrapassar o período de tempo pré-determinado para a regra; f. Deverá possuir mecanismo de classificação em tempo real dos sites visitados ou sistema de filtro de reputação que permita estabelecer uma reputação para cada endereço IP dos servidores de destino. A rede de reputação não deve somente ser

		baseada em informações de fluxo da própria base de appliances instalados, mas sim em correlações entre outros parâmetros: listas negras de URL, listas brancas de URL, listas de appliances comprometidos, volume global de trafego, histórico dos sites, dados de categorização de URLs e web crawlers; g. Não serão aceitas categorias pré-estabelecidas como Unrated, Uncategorized e afins, ou seja, é de responsabilidade do appliance categorizar automaticamente sites que não foram categorizados pelo fabricante anteriormente, realizando a análise do conteúdo do site e categorizando o mesmo de forma adequada; h. Permitir atualização automática da lista de URLs categorizadas via Internet por meio de base proprietária do fabricante do equipamento; i. Deverá permitir politicas baseadas em tempo (dias da semana, hora do dia) a fim de restringir acesso a horários pré-estipulados (ex.: horário comercial); j. Deverá possuir mecanismo de segurança que analise em tempo real a presença de conteúdo malicioso nas páginas acessadas. **5. MANIPULAÇÃO DE SITES:** a. Deverá suportar métodos de manipulação de sites dinâmicos e sites web 2.0, ou seja, alteração de seu comportamento, de modo tal que, por exemplo: • Redes Sociais (Facebook, Twitter, Instagram, Linked-in, atc.): Limitar acesso aos conteúdos ou recursos específicos dentro destes sites. • Seviços de compartilhameto de arquivos em nuvem (Google Drive, Microsoft OneDrive, etc.): bloquear ações de upload/download de arquivos. • Mensageiros instantâneos (WhatsApp, Telegram, etc.): Limitar acesso aos conteúdos ou recursos específicos dentro destes sites. **6. RELATÓRIOS:** a. Deverá possuir recursos que permita com que, a partir de informações como usuário e url, o sistema possa informar se o acesso será permitido ou negado e em que política ele passou ou o porquê foi bloqueado; b. Deverá possuir capacidade de listar todos os acessos ao proxy, permitindo a filtragem por, no mínimo, os campos Usuário/Ip/Categoria, exibindo informações como url acessada, categoria, política utilizada no acesso ou bloqueio; c. Deverá emitir relatórios do tipo Top 10 para: Usuário, Categorias, Url e Usuários Bloqueados; d. Deverá emitir relatórios por tipo da ameaça; e. Deverá exibir relatórios de atividades por usuário com os seguintes campos: site acessado, categorias, bloqueados e permitidos, consumo de banda; f. Deverá emitir relatórios customizáveis, produzindo documentos de múltiplos níveis; g. Deverá permitir a exportação dos dados dos relatórios para no mínimo dois dos seguintes formatos: CSV, XLS, PDF, HTML e TXT; h. Deverá possibilitar o agendamento de geração de relatório periódico e que o relatório seja exportado automaticamente para no mínimo dois destinos: e-mail, compartilhamento, FTP ou SCP.

		1. IMPLANTAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO
		
		a. A infraestrutura lógica de proxy presente hoje no TRE-PI é composta por:
		
		1. Proxy Web:
		  1. Responsável por atuar como intermediário entre o cliente e o servidor de destino externo;
		  2. Possui recursos para cache de conteúdo, autenticação de usuários e controle de acesso;
		  3. Utilizado para reduzir a quantidade de tráfego na rede, armazenando em cache solicitações frequentes;
		2. Proxy Reverso Interno:
		  1. Atua como intermediário entre os clientes e os servidores de destino internos;
		  2. É configurado para redirecionar solicitações para servidores específicos, balancear a carga entre vários servidores e proteger o servidor de destino contra ataques;
		3. Proxy Reverso Externo:
		  1. Atua como intermediário entre os clientes e os servidores de destino externos;
		  2. Utilizado para distribuição de carga e melhoria do desempenho dos

2	Requisitos do Projeto de Implantação da solução de TI	servidores; 3. É configurado para rotear as solicitações de acordo com as configurações definidas pelo administrador; b. Deverão ser configurados na solução todos os perfis de acesso via proxy existente na atual infraestrutura, que são compostas por 16 regras de acesso sendo: • 1 Regra de acesso a somente um grupo de sites delimitados; • 14 Regras de acesso para diferentes categorias de acesso à internet; • 1 Regra de acesso por cota de tempo. c. Deverá ser configurado 5 regras permitindo acesso a ranges de IP de forma anônima para a um grupo de sites da Internet. d. Na solução atual foi realizada a mudança de categoria a 130 sites localmente, caso estes sites estejam categorizados em categorias diferentes na nova solução, os mesmos deverão ser reconfigurados conforme ambiente atual. e. Deverá ser configurado 65 protocolos customizados a partir de um ou um grupo de portas. f. Deverão ser levantadas junto à equipe designada pela CONTRATANTE quais das novas funcionalidades que, embora não existam na solução atual, serão implantadas durante esta migração. Esta lista terá como limite todas as funcionalidades requeridas para o produto neste edital; g. Deverá ser proposta à equipe designada pela CONTRATANTE, as possíveis topologias (físicas e lógicas) da solução de Proxy de modo que atenda melhor a necessidade do TRE-PI diante do cenário encontrado, estando sujeito à aprovação e aceite da equipe designada da CONTRATANTE; h. Antes da execução dos serviços de implantação da solução proposta, deverá ser realizada uma reunião com a presença dos arquitetos da solução do fornecedor, os analistas da CONTRATANTE envolvidos no projeto e a equipe do Núcleo de Segurança de TI, para elaboração do plano do projeto para a implantação da solução, de forma a seguir as boas práticas de gerenciamento de projetos, incluindo: • Estudos de viabilidade, configuração, instalação e migração; • Detalhamento das atividades; • Escopo; • Cronograma; • Recursos; • Análise de riscos e impacto; • Plano de contingências; • Marcos do projeto; • Reuniões de acompanhamento, entre outros; • Documentação necessária. i. Todo o processo de migração da solução para a nova infraestrutura, instalação e configuração dos novos appliances é de responsabilidade da empresa CONTRATADA, devendo ser realizado por pessoal capacitado, comprovadamente certificado e autorizado pelo fabricante do equipamento adquirido, sob a supervisão da equipe designada da CONTRATANTE, que por sua vez deverão fornecer à empresa CONTRATADA as informações necessárias para tal; j. A instalação dos appliances adquiridos deve ser feita de forma paralela à infraestrutura atual e a migração para o novo núcleo deve acontecer de forma programada e definida pelos analistas da CONTRATANTE, com o mínimo possível de interrupção do funcionamento da solução atual, devendo toda e qualquer interrupção ser comunicada, programada e autorizada pela CONTRATANTE; k. Certificação final da solução, mediante testes de comunicação e apresentação de relatórios com os dados gerados. Os testes deverão compreender a comprovação de forma inequívoca do perfeito funcionamento dos mecanismos de alta disponibilidade, sejam eles de enlace físico, switches de acesso, switches core e também seus componentes. Todos estes testes deverão ser realizados com o acompanhamento da equipe de analistas da CONTRATANTE; l. Documentação As-Built de todo o projeto. m. O procedimento de instalação e configuração deve ser realizado em até 60 dias após a entrega dos appliances, que pode ser prorrogado em acordo aprovado pelo CONTRATANTE. **2. TESTE DE BANCADA** a. Deverão ser apresentados para o pleno atendimento aos requisitos deste edital e ainda em caráter eliminatório, testes de bancada, onde deverão ser comprovadas de forma prática, todas as características e funcionalidades descritas de cada

produto ou serviço deste edital. O teste de bancada deverá ser executado em ambiente de Produção da CONTRATANTE.

b. Após a energização, instalação e configuração inicial do equipamento, o fornecedor/fabricante terá um prazo de 40 (quarenta) horas para demonstrar as funcionalidades solicitadas.

3. MODELO DE PLANILHA DE ATENDIMENTO DE REQUISITO

a. O atendimento a todos os itens deve ser comprovado através de documentação oficial do fabricante da solução, que deverá ser anexada à proposta comercial ajustada. A instituição poderá realizar diligência junto ao fabricante para comprovar a autenticidade da documentação. A localização da comprovação na(s) página(s) deverá ser clara e precisa. O não atendimento destes requisitos implicará na desclassificação da proposta:

Item	Documento	Página	Localização

<table>
<tr>
<td>3</td>
<td>Requisitos da Garantia e Suporte</td>
<td>
a. O proponente e o fabricante deverão oferecer suporte técnico em língua portuguesa através de ligação telefônica gratuita do tipo 0800, que deve estar disponível no regime de 24 x 7 x 365 (24 horas por dia, 7 dias na semana e 365 dias no ano);

b. Os componentes da solução deverão ser fornecidos com garantia e suporte do fabricante de 36 (trinta e seis) meses, que deve estar disponível no regime de 24 x 7 x 365 (24 horas por dia, 7 dias na semana e 365 dias no ano), contados depois da assinatura do contrato, com atendimento on-site, com substituição do equipamento defeituoso ocorrendo em até no máximo 07 (sete) dias úteis após a abertura do chamado ou comprovação do defeito junto ao proponente/fabricante;

c. Atualizações de firmware e correções deverão estar disponíveis via Internet, sem custo adicional durante o período de garantia;

d. Em caso de falhas, fica a cargo do fornecedor o envio do produto substituto, e também é de responsabilidade do fornecedor devolver para o fabricante o produto danificado;

e. Os chamados de suporte técnico podem ser abertos com o proponente e com o suporte técnico do fabricante a critério da CONTRATANTE;

<table>
<tr><td>Nível de Severidade</td><td>Descrição</td><td>Email</td><td>On Site</td></tr>
<tr><td>Alto</td><td>Serviço completamente indisponível</td><td></td><td>02 horas</td></tr>
<tr><td>Médio</td><td>Serviço operando parcialmente</td><td></td><td>04 horas</td></tr>
<tr><td>Baixo</td><td>Serviço com degradação de desempenho ou funcionalidade</td><td>08 horas</td><td></td></tr>
<tr><td>Normal</td><td>Aplicação de patchs, hotfixes e firmware</td><td></td><td>Agendamento de 48 horas</td></tr>
</table>

f. Os chamados de severidade baixa, ou seja, aqueles que não afetam o desempenho da solução ou funcionalidades que não sejam de suma importância, deverão possuir um tempo de resposta máximo de 8h (oito horas) para diagnóstico e solução do problema, o mesmo deverá ser realizado por e-mail. Para solução do problema o SLA solicitado será apenas para hardware.

g. Os chamados de severidade média, ou seja, aqueles que influenciam negativamente no funcionamento de alguns dos seus serviços, mas sem torná-la totalmente inoperante, deverão possuir um tempo de resposta máxima de 4h (quatro horas) para diagnóstico e solução do problema, o mesmo deverá ser realizado On-Site. Para solução do problema o SLA solicitado será apenas para hardware.

h. Os chamados de severidade crítica, ou seja, aqueles relacionados a impactos de alta relevância que impedem a operação da solução, deverão possuir um tempo de resposta máximo de 02h (duas horas) para diagnóstico e solução do problema, o mesmo deverá ser realizado On Site. Para solução do problema o SLA solicitado será apenas para hardware.

i. Caberá exclusivamente à CONTRATANTE a categorização do chamado no ato da sua abertura.
</td>
</tr>
</table>

4	Requisitos de Capacitação	**TREINAMENTO OFICIAL DO FABRICANTE** a. Deverá ser realizado um treinamento oficial do fabricante da solução para até 08 (oito) participantes da equipe da CONTRATANTE; b. Este treinamento deverá ter no mínimo 20 (vinte) horas/aula de duração, e caso este treinamento não tenha em sua ementa, todas as funcionalidades exigidas neste edital, deve ser dado um novo treinamento oficial, o qual seu conteúdo abranja as funcionalidades restantes não contempladas no primeiro treinamento. c. O treinamento deve ser realizado em horário comercial, de segunda a sexta-feira; d. O treinamento deverá explanar conteúdo suficiente para a plena utilização dos produtos ofertados para a solução, devendo ser um curso de currículo oficial do fabricante, mesmo que extraordinariamente complementado pela cobertura das funcionalidades específicas destes produtos, bem como as características técnicas utilizadas para o desenho de toda a solução utilizada neste projeto, incluindo técnicas de resolução de problemas; e. Caso o conteúdo exigido não seja coberto por um único treinamento oficial, podem ser realizados tantos treinamentos oficiais quantos sejam necessários para que seja feito integralmente o repasse do conteúdo exigido, desde que obedecidos os mesmos prazos e condições estipulados neste documento; f. O treinamento deve ser ministrado por instrutores capacitados e possuidores de certificação emitida pelo fabricante da solução, bem como a instituição que realizará o treinamento deve possuir certificação de capacitação fornecida pelo fabricante específica para execução de treinamentos; g. Deverá ser agendado a critério da CONTRATANTE, com antecedência de 30(trinta) dias consecutivos para o perfeito planejamento junto ao centro autorizado. Após o agendamento, o treinamento deve ser iniciado em até 60 (sessenta) dias consecutivos; h. A CONTRATANTE se reserva o direito de indicar, em cada solicitação de treinamento, o número de 01 (um) até 08 (oito) participantes, sendo que a soma de todos os participantes não ultrapassará o total de 08 (oito); i. O treinamento pode ser ministrado nas modalidades online ao vivo (EAD), podendo ser gravado, a critério da CONTRATANTE. j. O licitante vencedor deve se responsabilizar em fornecer, sem custo adicional para a CONTRATANTE, local de treinamento, infraestrutura e material didático impresso na língua portuguesa (Brasil) ou língua inglesa a todos participantes para acompanhamento do treinamento; k. Ao final de cada treinamento deve ser emitido e entregue a cada aluno certificado oficial de participação, emitido pelo próprio fabricante; l. A entrega dos certificados oficiais de participação é condição necessária ao pagamento dos treinamentos. m. O treinamento passará por avaliação de satisfação no âmbito de instrutor e de conteúdo do curso, o mesmo será realizado por documento interno da CONTRATANTE e servira como avaliação do treinamento. n. As avaliações de satisfação deverão ser superioras a 70% para o pagamento dos treinamentos.
5	Requisitos de Experiência Profissional da Equipe Técnica	a. A implantação deve ser realizada por profissionais certificados, que possuam certificação do fabricante da solução adquirida ou pelo próprio fabricante, que lhes confiram as competências necessárias para a realização dos respectivos serviços. b. Para esta solução é necessária a capacitação do corpo técnico e implementação com acompanhamento de um profissional especializado na solução e/ou pelo próprio fabricante, por se tratar de uma solução complexa. c. A proponente deverá possuir pelo menos 1 (um) profissional capacitado com certificação, e deverá apresentar certificado técnico da solução durante a fase de habilitação. d. Os profissionais que inicialmente manterão relacionamento direto com o CONTRATANTE deverão ser apresentados após assinatura do CONTRATO na REUNIÃO INICIAL, ocasião em que deverão ser entregues as comprovações dos perfis exigidos. A apresentação de novos profissionais durante a execução do CONTRATO, incluindo a entrega das comprovações dos perfis à equipe de fiscalização do CONTRATO, deverá ser feita previamente ao início da atuação destes.

6	Requisitos de Formação da Equipe Técnica	a. O profissional que atuará como gerente de projeto deve ter certificação como Project Management Professional (PMP); b. O Contratado deverá apresentar profissional(is) com certificação técnica emitida pelo fabricante ou instituto autorizado pelo respectivo fabricante do Secure Web Gateway, indicando sua habilitação técnica na tecnologia ofertada. Este profissional deve executar "in loco" os serviços especificados e prestar o suporte e o atendimento em garantia dos produtos
7	Requisitos da Metodologia de trabalho	Não se aplica
8	Requisitos de Segurança sob o ponto de vista Técnico	Não se aplica

5.4 – Outros requisitos

ID	TIPO	REQUISITO
1		
...		

6. IDENTIFICAÇÃO DAS SOLUÇÕES DISPONÍVEIS

SOLUÇÃO 1	**NOME DA SOLUÇÃO:**	Utilização de ferramentas Open Source (Squid, pfSense, OPNsense, etc.)
	DESCRIÇÃO:	Implantação de solução Open Source para filtragem e otimização de conteúdo web, p. ex., Squid, pfSense, OPNsense e semelhantes.
	FORNECEDOR(ES):	Diversos.
	ENTIDADE:	
	VALOR:	R$ 0,00
SOLUÇÃO 2	**NOME DA SOLUÇÃO:**	Aquisição de ferramenta proprietária
	DESCRIÇÃO:	Implantação de solução proprietária para filtragem e otimização de conteúdo web.
	FORNECEDOR(ES):	Cisco, Forcepoint, Check Point, Symantec, McAfee, etc.
	ENTIDADE:	
	VALOR:	R$ 1.292.066,93

7. DETALHAMENTO DAS SOLUÇÕES E ALTERNATIVAS EXISTENTES

REQUISITO	ID DA SOLUÇÃO	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	X		
	2	X		
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Eleitoral?	1	X		
	2	X		
A Solução está disponível no Portal do Software Público Brasileiro?	1	X		
	2		X	
A Solução é um software livre ou software público?	1	X		
	2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1	X		
	2	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1	X		
	2	X		
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus?	1			X
	2			X

8. ANÁLISE E COMPARAÇÃO DOS CUSTOS TOTAIS DA DEMANDA

Ao ser considerada a implementação de uma solução de Secure Web Gateway (SWG) na infraestrutura de TI deste Tribunal, duas abordagens principais surgem como opções viáveis: a Solução 1, que envolve a utilização de ferramentas open source, como Squid, pfSense, OPNsense e outros, e a Solução 2, que se baseia na aquisição de uma ferramenta proprietária.

Cada uma dessas soluções possui vantagens e desvantagens que devem ser cuidadosamente avaliadas antes de tomar uma decisão.

Solução 1: Utilização de Ferramentas Open Source (Squid, pfSense, OPNsense, etc.)

A principal vantagem das ferramentas open source é o custo reduzido. Elas não envolvem licenciamento ou taxas de aquisição, o que as torna economicamente mais acessíveis. Além disso, a natureza open source permite personalização de acordo com as necessidades do Tribunal. As comunidades ativas em torno dessas ferramentas fornecem suporte e solução de problemas, e a transparência é uma característica positiva devido à disponibilidade do código fonte.

No entanto, há desafios a considerar. O suporte pode ser limitado em comparação com soluções proprietárias que oferecem suporte técnico profissional. A complexidade da configuração e manutenção pode ser consideravelmente maior, exigindo um conhecimento técnico avançado. A integração com outros sistemas empresariais também pode ser mais desafiadora.

Solução 2: Aquisição de Ferramenta Proprietária

Ferramentas proprietárias oferecem suporte profissional, funcionalidades avançadas e integração simplificada com outros sistemas do Tribunal. A configuração e operação tendem a ser mais simples, o que reduz a carga de trabalho da equipe de TI.

No entanto, essas vantagens vêm com contrapartidas que devem ser consideradas, incluindo custos financeiros com taxas de licenciamento, aquisição e manutenção da solução, assim como a vinculação ao suporte contínuo e atualizações oferecidos pelo fornecedor. A flexibilidade para personalizar a ferramenta pode ser limitada em comparação com soluções open source, e a transparência pode ser uma preocupação devido à natureza proprietária.

Decisão: Solução 2 (Aquisição de Ferramenta Proprietária)

Apesar das vantagens que as soluções open source apresentam, **a escolha pela Solução 2, Aquisição de Ferramenta Proprietária, é recomendada**. Isso se deve principalmente ao suporte profissional, funcionalidades avançadas e integração simplificada oferecidos pelas ferramentas proprietárias.

Embora haja um investimento financeiro inicial mais significativo, esses benefícios podem resultar em uma implementação mais eficaz, gerenciamento simplificado e melhor proteção dos ativos digitais do Tribunal. Além disso, a dependência do fornecedor é contrabalanceada pelo suporte especializado e atualizações regulares que garantem a segurança contínua da solução.

Em última análise, a escolha entre essas soluções depende das necessidades específicas, dos recursos disponíveis e das prioridades do TRE-PI em termos de segurança, custo e eficiência operacional.

Argumentação a Favor de Appliances Físicos ou Virtuais em Vez de Soluções SaaS para Implantação de uma Solução de SWG no Setor Público

Implantar uma solução de Secure Web Gateway (SWG) no setor público requer uma análise cuidadosa das opções disponíveis. Embora soluções baseadas em Software as a Service (SaaS) tenham ganhado popularidade nos últimos anos devido à sua facilidade de uso e manutenção, há razões convincentes para preferir appliances físicos ou virtuais na implantação de uma solução de SWG no setor público.

a. Controle Total sobre os Dados e a Segurança: Proteger dados sensíveis é uma preocupação primordial no setor público. Ao utilizar appliances físicos ou virtuais, a agência governamental tem controle total sobre a localização e o armazenamento dos dados, reduzindo o risco de exposição a terceiros.

b. Requisitos de Conformidade: As agências governamentais frequentemente estão sujeitas a regulamentações rigorosas em relação à segurança de dados e à privacidade. Utilizar uma solução de SWG instalada internamente oferece mais flexibilidade para personalizar e ajustar a infraestrutura de acordo com os requisitos específicos de conformidade.

c. Personalização e Controle sobre Políticas de Segurança: O setor público pode ter necessidades de segurança muito específicas que não são facilmente atendidas por soluções SaaS genéricas. Com um appliance físico ou virtual, é possível personalizar as políticas de segurança para atender às necessidades exclusivas da agência.

d. Disponibilidade e Desempenho: Garantir o desempenho é crucial para o funcionamento contínuo dos serviços governamentais. Em muitos casos, as soluções de SWG baseadas em appliances físicos ou virtuais podem ser dimensionadas e configuradas para garantir um desempenho consistente, mesmo sob cargas pesadas de tráfego.

e. Continuidade de Serviços e Resiliência: As soluções de appliances físicos ou virtuais permitem a implementação de estratégias de redundância e backup para garantir a continuidade dos serviços em caso de falhas de hardware ou desastres naturais.

f. Considerações de Custos a Longo Prazo: Embora as soluções SaaS possam parecer mais econômicas a curto prazo, os custos podem aumentar substancialmente ao longo do tempo à medida que a agência depende cada vez mais da plataforma. Em contrapartida, os custos de manutenção e atualização de um appliance físico ou virtual geralmente são mais previsíveis.

g. Segurança Cibernética e Soberania de Dados: Dependendo das leis e regulamentações locais, as agências governamentais podem ter restrições quanto à localização dos dados. A utilização de uma solução de SWG interna oferece um maior controle sobre a soberania dos dados.

Em resumo, ao escolher entre appliances físicos ou virtuais e soluções SaaS para a implantação de uma solução de SWG no setor público, o controle, a personalização, a conformidade e a segurança são fatores críticos que tornam as primeiras opções mais atraentes. Embora soluções SaaS tenham suas vantagens, as considerações exclusivas do setor público frequentemente favorecem a manutenção de um controle direto sobre a infraestrutura de segurança.

A seguir evidencia-se a pesquisa de preços realizada tendo em vista a Solução 2 (Aquisição de Ferramenta Proprietária) sugerida:

OBSERVAÇÕES IMPORTANTES:

1. Foram feitas tentativas de contato com diversos fornecedores de ferramentas proprietárias de SWG, porém apenas duas empresas

responderam e estabeleceram diálogo de manera mais acertiva.
2. Também foi feita uma extensa pesquisa à base de dados de compras governamentais (ComprasNet, Painel de Preços, ConecteJus, portais de diversas instituições, etc.), porém a aquisição mais recente encontrada que se enquadrava nas demandas do presente ETP data de Fevereiro de 2021.

1) PROPOSTA 01: **CHECK POINT HARMONY CONNECT INTERNET ACCESS** (SEI Nº 0001909416)

ITEM	DESCRIÇÃO	QTDE	VALOR UNITÁRIO	VAOR TOTAL
01	Solução de Harmony Connect Internet Access Harmony Secure Internet Access- service for one user for 3 years.	1500	R$ 497,94	R$ 746.910,00
02	Suporte Premium do Fabricante	1	R$ 52.281,12	R$ 52.281,12
03	Implantação e configuração Remota da solução Harmony Connect / Passagem de Conhecimento	1	R$ 67.500,00	R$ 67.500,00
				R$ 866.691,12

2) PROPOSTA 02: **FORCEPOINT WEB SECURITY ADVANCED MALWARE DETECTION** (SEI Nº 0001909421)

ITEM	DESCRIÇÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
1	Forcepoint Web Security e Advanced Malware Detection para 36 meses	1500	R$ 1.066,34	R$ 1.599.506,48
2	Suporte e Instalação	1	R$ 60.000,00	R$ 60.000,00
3	Treinamento	1	R$ 30.000,00	R$ 30.000,00
				R$ 1.689.506,48

3) PESQUISA DE PREÇOS 01: CONTRATO BRB 034/2021 - BANCO DE BRASÍLIA S.A. (SEI Nº 0001909427)

ITEM	DESCRIÇÃO	QTDE	UNIDADE	VALOR UNIDADE	VALOR TOTAL
1	Secury Web Gateway - licença 1500	01	Licença	R$ 672,12	R$ 1.008.187,20
2	Treinamento	01	Turma	R$ 29.000,00	R$ 29.000,00
3	Suporte	36	Mensal	R$ 7.856,00	R$ 282.816,00
					R$ 1.320.003,20

Desse modo, o Valor Total Médio da Solução 2 (Aquisição de Ferramenta Proprietária) sugerida foi calculado em **R$ 1.292.066,93 (um milhão, duzentos e noventa e dois mil sessenta e seis reais e noventa e três centavos).**

9. SOLUÇÃO ESCOLHIDA

9.1 – Identificação

NOME:	Aquisição de ferramenta proprietária		
JUSTIFICATIVA:	Apesar das vantagens que as soluções open source apresentam, a escolha pela Solução 2, Aquisição de Ferramenta Proprietária, é recomendada. Isso se deve principalmente ao suporte profissional, funcionalidades avançadas e integração simplificada oferecidos pelas ferramentas proprietárias. Embora haja um investimento financeiro inicial mais significativo, esses benefícios podem resultar em uma implementação mais eficaz, gerenciamento simplificado e melhor proteção dos ativos digitais do Tribunal. Além disso, a dependência do fornecedor é contrabalanceada pelo suporte especializado e atualizações regulares que garantem a segurança contínua da solução.		
DESCRIÇÃO:	Implantação de solução proprietária para filtragem e otimização de conteúdo web.		
BENS E	**ID**	**BEM / SERVIÇO**	**VALOR ESTIMADO**
	1	Licença de Solução de Secure Web Gateway para 1.500 usuários	R$ 1.118.201,23

SERVIÇOS	2	Instalação e Suporte por 36 meses	R$ 131.699,04
	3	Treinamento	R$ 42.166,66
			R$ 1.292.066,93

9.2 – Alinhamento com as necessidades de negócio

ID	FUNÇÃO	NECESSIDADE DO NEGÓCIO
1	A solução escolhida atende às necessidades quando contribui no alcance do objetivo estratégico "Aprimorar os mecanismos de transparência, segurança da informação e acesso à informação", constante no PEI do TRE-PI.	Possibilitar segurança da informação.
2	Atende às necessidades de TIC quando contribui para melhorar o objetivo estratégico "Garantir a disponibilidade dos serviços de TIC essenciais às atividades judiciais e administrativas" e o indicador 7 "Índice de disponibilidade de serviços essenciais de TIC", constantes	Possibilitar continuidade dos serviços.

9.3 – Benefícios esperados

ID	TIPO	BENEFÍCIOS
1	Segurança	Aumento da resiliência a ciberataques nos serviços de TI.
2	Desempenho	Aumentar o nível de eficiência de uso dos canais de comunicação.
3	Segurança	Aumentar o grau de proteção contra códigos maliciosos (ou malware).
4	Produtividade	Aumentar o nível de produtividade dos recursos humanos empregados pelo Poder Judiciário
5	Desempenho	Reduzir os custos com canais de comunicação de dados.

9.4 – Justificativa de não-conformidade

ID	SOLUÇÃO	JUSTIFICATIVA
1	Utilização de ferramentas Open Source (Squid, pfSense, OPNsense, etc.)	Suporte limitado em comparação com soluções proprietárias que oferecem suporte técnico profissional. Alta complexidade da configuração, manutenção e integração com outros sistemas, exigindo conhecimento técnico avançado.

10. AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO PARA EXECUÇÃO CONTRATUAL

ID	TIPO DE NECESSIDADE	SIM	NÃO	DESCRIÇÃO
1	Infraestrutura Tecnológica	X		A solução deverá prover as funcionalidades de Proxy HTTP/HTTPS, Filtro de Conteúdo, Caching e AntiMalware, incluindo e inspeção de tráfego SSL e Monitoramento de camada quatro do modelo OSI; A solução deve ser totalmente compatível com infraestrutura computacional hiperconvergente baseada em tecnologia VMWare.
2	Infraestrutura Elétrica		X	Não se aplica.
3	Logística de implantação	X		A instalação dos appliances adquiridos deve ser feita de forma paralela à infraestrutura atual e a migração para o novo núcleo deve acontecer de forma programada e definida pelos analistas da CONTRATANTE, com o mínimo possível de interrupção do funcionamento da solução atual, devendo toda e qualquer interrupção ser comunicada, programada e autorizada pela CONTRATANTE.
4	Espaço Físico		X	Não se aplica.
5	Mobiliário		X	Não se aplica.
6	Impacto ambiental		X	Não se aplica.

11. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

DESCRIÇÃO DOS RECURSOS NECESSÁRIOS PARA SUPORTAR A CONTRATAÇÃO DA SOLUÇÃO		
11.1. Recursos Materiais		
Item	**Descrição**	
1	Não se aplica.	
11.2. Recursos Humanos		
Item	**Função**	**Formação**
1	Técnico	Conhecimento de redes. Conhecimento em segurança da informação. Capacitação na solução adquirida.

12. ESTRATÉGICA DE CONTINUIDADE CONTRATUAL

IDENTIFICAÇÃO DE EVENTOS QUE POSSAM CAUSAR INTERRUPÇÃO CONTRATUAL			
Evento	**Descrição**	**Ação de Contingência**	**Responsável**
1	Defeito em equipamento	Implementação da solução em cluster ou substituição.	Equipe de planejamento
2	Fim do período do suporte e garantia técnica	Deliberação acerca da necessidade de nova contratação da garantia técnica da solução para upgrade e/ou renovação das licenças e suporte da solução.	STI

13. AÇÕES PARA TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

Item	Ação	Responsável	Data Início	Data Fim
1	Decisão por nova aquisição ou contratação de extensão de suporte	STI		

14. ESTRATÉGIA DE INDEPENDÊNCIA

14.1. Transferência de Conhecimento Tecnológico		
Item	**Informações que deverão ser transmitidas pela Contratada**	**Forma de transferência do Conhecimento**
1	Treinamento da solução, cujo escopo cubra conceitos de configuração, operação, administração, gerência, otimização, resolução de problemas e gestão de todos os componentes da solução, de forma que os participantes capacitados possam colocar a solução em produção, bem como planejar mudanças de configuração no ambiente.	Treinamento ao vivo na modalidade de Ensino a Distância.
...		
14.2. Direitos de Propriedade Intelectual e Autorais		
Item	**Cláusulas segundo a lei Nº 9.610, de 19 de fevereiro de 1998.**	
1	O instrumento contratual deve estabelecer que os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados, pertençam à Administração;	
2	A Contratada deverá ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração.	

15. ANÁLISE DE RISCOS

15.1 – Riscos do processo de contratação (identificar os riscos que podem comprometer o processo de contratação, resultando em atrasos ou em comprometimento do processo de contratação – IN04, art. 16, I)

RISCO 1	PROBABILIDADE
Total entendimento do edital.	(X) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto

ID	EFEITO	IMPACTO	AÇÃO DE RESPOSTA AO RISCO	TIPO DE AÇÃO	RESPONSÁVEL	ÁREA
1	Não compreensão de todas as cláusulas, fases, entregas, características, obrigações do edital	(X) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Realização de reuniões de alinhamento total com todas as partes envolvidas no projeto	(X) 1-Mitigação ( ) 2-Contingência	Contratada	STI/SAOF

RISCO 2					PROBABILIDADE	
Atraso na entrega dos produtos.					(X) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	- Atraso na fabricação dos produtos - Atraso no transporte dos produtos para embarque aéreo na origem - Greve da Receita Federal - Greve na INFRAERO - Atraso no transporte dos produtos após o desembarque aéreo no destino	( ) 1-Baixo (X) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	- Realização de reuniões de alinhamento total com todas as empresas subcontratadas das quais depende o sucesso na execução do projeto - Realização de reuniões de alinhamento total com todos os fornecedores das quais depende o sucesso na execução do projeto	(X) 1-Mitigação ( ) 2-Contingência	Contratada	STI/SAOF

15.2 – Riscos da solução de TI escolhida (identificar os riscos que podem fazer com que, após o serviço ter sido contratado, o mesmo não atenda às necessidades do negócio especificadas – IN04, art. 16, II)

RISCO 1					PROBABILIDADE	
Impacto na performance e usabilidade da rede de dados.					( ) 1-Baixo (X) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**DANO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	- Depreciação da performance e usabilidade de navegação dos usuários na Internet e Intranet do TRE-PI.	( ) 1-Baixo (X) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	- Configuração adequada dos parâmetros da solução, possibilitando a máxima eficiência com o menor impacto possível no ambiente.	(X) 1-Mitigação ( ) 2-Contingência	Contratada/Contratante	STI/SEINF

16. ESTRATÉGIA PARA CONTRATAÇÃO

16.1. SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (Res. CNJ 182/2013, art. 16)

16.1.1 – DEFINIÇÃO (NATUREZA DO OBJETO) DA SOLUÇÃO (critérios que serão usados para definir o tipo de contratação, modalidade de licitação, etc: inovação tecnológica ou serviço/bem comum; necessidade pontual ou contínua- Res. CNJ 182/2013, art. 16, IV)	
Critério	**Atendimento da Solução**
É possível especificar o serviço usando parâmetros usuais de mercado?	Sim.
É possível medir o desempenho da qualidade usando parâmetros usuais de mercado?	Sim.
O objeto da contratação se estende necessariamente por mais de um ano?	Sim. Os serviços de garantia e suporte técnicos das soluções se estendem por mais de um ano, pois são necessários para a estabilidade, economia de custos, previsibilidade orçamentária, redução de sobrecarga administrativa, conformidade regulatória e garantia de atualizações consistentes, o que caracteriza a sua natureza continuada.
O objeto da contratação é essencial para o negócio?	Sim. A disponibilização de serviços via WEB é fundamental para a implementação do Plano de Transformação Digital. Nesse sentido, se faz necessário que essa disponibilização ocorra com níveis mínimos de segurança e disponibilidade

16.1.2 – PARCELAMENTO E ADJUDICAÇÃO DA CONTRATAÇÃO (justificar se é técnica e economicamente viável dividir a solução a ser contratada. Informar se o objeto pode ou não ser dividido em itens ou até mesmo em grupos. Em caso de divisão, verificar se há prejuízo nos resultados finais a serem obtidos. De acordo com o parcelamento do objeto, informar se a adjudicação pode ou não ser realizada para mais de um fornecedor. Justificar a escolha. Esse item não se aplica aos casos de Dispensa ou Inexigibilidade - (Res. CNJ 182/2013, art. 16, II e III).
A aquisição se dará por adjudicação global não sendo possível seu parcelamento. Devido necessidade de redundância, alta disponibilidade e ponto de gerenciamento único, não é possível a aquisição de equipamentos de marcar/modelos distintos.

16.2. RESPONSABILIDADES DA CONTRATANTE E DA CONTRATADA

16.2.1 – DEVERES E RESPONSABILIDADES DA CONTRATANTE (deveres e responsabilidades da contratante que comporão o contrato)	
ID	**Dever / Responsabilidade**
1	Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos. Anotar em registro próprio os defeitos detectados e comunicando as ocorrências de quaisquer fatos que, a seu critério, exijam o reparo ou substituição dos bens por parte da CONTRATADA. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo. Abrir e acompanhar os chamados técnicos à contratada, elaborando relatórios mensais, constando as conformidades e desconformidades dos serviços prestados. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado. Atestar a(s) notas fiscal(ais) apresentada(s) pela CONTRATADA após o recebimento definitivo dos equipamentos, conforme especificações descritas neste Termo de Referência. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos. Prestar informações e esclarecimentos que venham a ser solicitados pela CONTRATADA, necessários à execução do contratado.

16.2.2 – DEVERES E RESPONSABILIDADES DA(S) CONTRATADA(S) (deveres e responsabilidades da(s) contratada(s) que comporão o contrato. A(s) contratada(s) não poderá(ão) se eximir dessas responsabilidades, mesmo havendo subcontratação - (IN04, art. 15, II)	
ID	**Dever / Responsabilidade**

1	A CONTRATADA obriga-se a fornecer o material obedecendo rigorosamente às especificações discriminadas no Termo de Referência. Manter, durante o fornecimento, todas as condições de habilitação e qualificação exigidas no Termo de Referência. Não transferir a outrem, no todo ou em parte, o objeto do contrato a ser firmado. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo e prazo de garantia. Atender aos chamados técnicos no prazo estipulado pela contratante. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990). Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência (item 9.2.3), o objeto com avarias ou defeitos. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação. Responsabilizar-se integralmente pelo fiel cumprimento do objeto contratado, prestando todos os esclarecimentos que forem solicitados pela CONTRATANTE, cujas reclamações se obriga a atender. Apresentar o Termo de Confidencialidade e Sigilo (Anexo I) dos envolvidos na implantação da solução, migração de dados e operação assistida. Prover assistência técnica no **território** brasileiro. **Dar garantia não inferior a 36 (trinta e seis) meses, a contar da data de emissão do Termo de Recebimento Definitivo.**

16.3 INDICAÇÃO DOS TERMOS CONTRATUAIS (IN04, art. 15, III)

16.3.1 – PROCEDIMENTOS E CRITÉRIOS DE ACEITAÇÃO (IN04, art. 15, III, a)			
ID	**Etapa / Fase / Item** (em qual etapa, fase ou item do projeto será aplicada a mensuração)	**Indicador** (qual será o indicador mensurado. Qual será a unidade de medida a ser avaliada)	**Valor Mínimo Aceitável** (valor mínimo aceitável daquele item de mensuração)
1	Aceitação da proposta	Configurações dos equipamentos/serviços ofertados	Especificação mínima exigida em edital.
2	Implantação da solução	Carga horária do treinamento	Carga horária mínima de 20 horas.
3	Recebimento definitivo	Adequação dos equipamentos/serviços	Especificação mínima exigida em edita.
4	Recebimento definitivo	Garantia dos equipamentos	Garantia de 36 (trinta e seis) meses.
5	Recebimento definitivo	Suporte dos softwares/licenças entregues	Suporte de 36 (trinta e seis) meses.

16.3.2 – FORMA DE PAGAMENTO (modo ou percentual que será pago por cada entrega em função do resultado a ser obtido -IN04, art. 15, III, e)

O pagamento será efetuado por meio de depósito bancário em conta corrente, até o 10º (décimo) dia útil a partir da emissão do Termo de Aceite Definitivo, devidamente certificada pela equipe de contratação e processada na forma da legislação vigente.

O pagamento relativo ao banco de horas para suporte/consultoria será realizado até o 10º (décimo) dia útil a partir da entrega da fatura de serviço, considerando-se os chamados abertos e encerrados dentro do mês de referência.

16.3.3 – CRONOGRAMA DE EXECUÇÃO FÍSICO-FINANCEIRA (IN04, art. 15, III, f)

ID	**Entrega** (listagem do item ou serviço a ser entregue. Esta entrega pode ser parcelada ou integral)	**Data de Entrega**	**Percentual a ser Pago**
1	*Secure Web Gateway* (SWG)	Até 90 (noventa) dias após recebimento da ordem de serviço.	100%
Total:			

16.3.4 – MECANISMOS FORMAIS DE COMUNICAÇÃO (IN04, art. 15, III, g)

Função de Com. 1 (listagem do que deverá ser contemplado neste mecanismo de comunicação):	Assinatura de contrato, emissão de ordem de fornecimento, emissão de notas fiscais.			
Documento (nome do documento a ser entregue)	**Emissor**	**Destinatário**	**Meio** (forma com que o documento deverá ser produzido e entregue)	**Periodicidade** (frequência que os documentos deverão ser emitidos e entregues pela contratada ou pela administração)
Ata de Registro de Preços	Contratante	Contratada	Eletrônico	1 vez
Contrato	Contratante	Contratada	Eletrônico	1 vez
Ordem de Fornecimento	Contratante	Contratada	Eletrônico	1 vez para cada unidade do item 1, considerando a disponibilidade orçamentária.
Nota Fiscal	Contratada	Contratante	Físico / Eletrônico	Uma única vez a cada Ordem de Fornecimento
Nota de Empenho	Contratante	Contratada	Eletrônico	Uma única vez a cada Ordem de Fornecimento
Abertura de chamado	Contratante	Contratada	Eletrônico	Mensalmente, sempre que houver chamado concluído no mês de referêcia

16.3.5 – REGRAS PARA APLICAÇÃO DE MULTAS E SANÇÕES (IN04, art. 15, III, h)

ID	**Ocorrência** (descrição clara das situações em que se caracterizará a infração a algum termo contratual. Devem ser descritas as não conformidades, ou outras situações ou ocorrências em que serão propostas sanções a serem aplicadas pela Área Administrativa)	**Sanção / Multa** (descrição da sanção/multa a ser aplicada de acordo com cada situação ou ocorrência listada. As multas e sanções devem ser proporcionais ao impacto que a ocorrência provocará no órgão e aos casos de reincidência das ocorrências)
1	• Não assinar o contrato ou Ata de Registro de Preços • Deixar de entregar documentação exigida neste edital; • Apresentar documentação falsa; • Não manter a proposta; • Falhar ou fraudar na execução do contrato; • Comportar-se de modo inidôneo; • Fazer declaração falsa; • Cometer fraude fiscal.	Fundamentado no artigo 7º da Lei 10.520/2002, regulamentado pelo artigo 49 do Decreto n.º 10.024/2019, ficará impedido de licitar e contratar com a União e será descredenciado no SICAF, pelo prazo de até 05 (cinco) anos, garantido o direito à ampla defesa.
2	Faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante.	Penalidade de advertência.
3	• Atraso no cumprimento das obrigações assumidas contratualmente, que tenha acarretado prejuízos financeiros para o TRE-PI; • Entrega de objeto, em desacordo com a proposta aceita pela Contratante, sem prejuízo das demais sanções	Suspensão temporária de participação em licitação e impedimento de contratar com o TRE-PI, p**or até 1 (um) ano,** se, por culpa ou dolo, prejudicar ou tentar prejudicar a execução do Contrato

4	• Entrega de objeto falso, seja como amostra ou como bem a ser entregue por ocasião de emissão de ordem de fornecimento, assim entendido, aquele em que houve manipulação para aparentar ser de outra marca/fabricante, ou ter características que originalmente não lhe pertençam, sem prejuízo das demais medidas cabíveis; • Não atendimento à solicitação de troca ou prestação de garantia do objeto, quando solicitado pela Contratante, no prazo fixado no edital • Cometimento de quaisquer outras irregularidades que acarretem prejuízo ao TRE-PI, ensejando a rescisão do Contrato por culpa da CONTRATADA; • Apresentação, ao TRE-PI, de qualquer documento falso ou falsificado, no todo ou em parte, com o objetivo de comprovar, durante a execução do Contrato, a manutenção das condições apresentadas na habilitação	Suspensão temporária de participação em licitação e impedimento de contratar com o TRE-PI, p**or até 2 (dois) anos,** se, por culpa ou dolo, prejudicar ou tentar prejudicar a execução do Contrato
5	Entrega do objeto com atraso	Multa moratória mensurada na forma de tabela a ser prevista no termo de referência, até o limite de 13% (treze por cento), calculada sobre o valor do objeto em atraso
6	Inexecução total do contrato	Multa compensatória de 15% (quinze por cento) sobre o valor do objeto

16.4. CRITÉRIOS TÉCNICOS DE JULGAMENTO DAS PROPOSTAS (IN04, art. 15, VII)

16.4.1 – CRITÉRIOS DE SELEÇÃO			
( ) Licitação (X) Registro de Preço ( ) Dispensa de licitação ( ) Inexigibilidade de licitação			
Modalidade:	Pregão Eletrônico	**Tipo:**	Menor Preço global
Justificativa: (obrigatório se for dispensa ou inexigibilidade de licitação)	O objeto da contratação pretendida possui requisitos de desempenho e qualidade objetivamente definidos por meio de especificações usuais de mercado, razão por que se entende adequada a utilização do Pregão Eletrônico. Considerando a incerteza de disponibilidade de recursos orçamentários para a aquisição da totalidade da demanda indicada no presente exercício financeiro, bem como a possível expansão da solução em função do crescimento da demanda, através da adesão de outros Regionais, entende-se necessária a realização de Pregão Eletrônico com Sistema de Registro de Preços, conforme o art. 3º do Decreto Nº 7.892/2013.		

16.5. INDICAÇÃO DA EQUIPE DE GESTÃO DA CONTRATAÇÃO (ou comissão de recebimento de bens) (Res. CNJ 182/2013, art. 16, VIII)

Gestor do Contrato:	Rosemberg Maia Gomes	Telefone:	
E-mail do Gestor do Contrato:		Setor:	
Fiscal Demandante:	Rosemberg Maia Gomes	Telefone:	
E-mail do Fiscal Demandante:		Setor:	
Fiscal Técnico:	Aciel Sousa Mendes	Telefone:	
E-mail do Fiscal Técnico:		Setor:	
Fiscal Administrativo:	Gleidson Cavalcanti de Lima	Telefone:	
E-mail do Fiscal Administrativo:		Setor:	

17. ASSINATURAS

INTEGRANTE	NOME	ÁREA
Demandante:	Rosemberg Maia Gomes	STI
Técnico:	Aciel Sousa Mendes	STI
Administrativo:	Gleidson Cavalcanti de Lima	SAOF

Teresina, 13 de abril de 2023.

Documento assinado eletronicamente por **Gleidson Cavalcanti de Lima**, **Técnico Judiciário**, em 18/09/2023, às 13:58, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Aciel Sousa Mendes**, **Técnico Judiciário**, em 18/09/2023, às 14:13, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0001812006** e o código CRC **52FB2415**.

--