SISTEMA DE COMPRAS, LICITAÇÕES, CONTRATOS E INSTRUMENTOS CONGÊNERES
ESTUDO TÉCNICO PRELIMINAR - ETP

Estudo Técnico Preliminar - ETP Nº 2063905/2024 - SECRETARIA DE TECNOLOGIA DA INFORMACAO

Conforme processo eletrônico nº 7002307-71.2021.8.08.0000, as contratações devem ser precedidas de Estudos Técnicos Preliminares (ETP's), atendendo ao disposto na Lei nº 14.133/2021 e na Instrução Normativa nº 40/2020, tal como estabelece a Norma Introdutória NP 01.

Objetivando subsidiar a elaboração do ETP, importante examinar os normativos (normas, regras, preceitos e legislações) que disciplinam os materiais/equipamentos a serem adquiridos, de acordo com sua natureza, além de analisar as aquisições anteriores do mesmo objeto, a fim de identificar as inconsistências ocorridas nas fases de planejamento da contratação, seleção do fornecedor e recebimento e utilização dos materiais/equipamentos.

Orientações para elaboração do Estudo Técnico Preliminar, encontram-se disponíveis na Intranet do PJES, em "Norma de Procedimentos" - Formulários da NP 01 - Sistema de Compras, Licitações e Contratos.

1- INFORMAÇÕES BÁSICAS:

Número do processo administrativo:

7003203-46.2023.8.08.0000 - Contratação de sistema unificado de proteção de borda (Firewall), incluindo fornecimento de licença, transferência de conhecimento, suporte, instalação, implantação, garantia e treinamento para o PJES.

Área requisitante:

Secretaria de Tecnologia da Informação

2- DESCRIÇÃO DA NECESSIDADE DE AQUISIÇÃO:

A realidade que o Poder Judiciário Nacional está inserida atualmente traz consigo a absoluta necessidade do uso dos mais novos recursos de tecnologia da informação e comunicação (TIC), e dentre eles, o fornecimento de solução de segurança da informação (Firewall) para proteção de acesso à rede do PJES.

A necessidade da contratação dessa solução, se estampa em dois objetivos estratégicos do Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETI) – TJES: Garantir a disponibilidade de sistemas de TIC essenciais ao judiciário e Promover a segurança da informação. Esta última é alcançada com base na ação sugerida pela PETI: Investir em segurança de TIC, especialmente com aquisição de equipamentos, sistemas e formação profissional.

Atualmente, o sistema de proteção de perímetro não satisfaz completamente a demanda de tráfego de rede do PJES e não suporta o crescimento a curto prazo, pois já apresenta sinais de sobrecarga, que cresceram exponencialmente com as novas soluções de TIC disponibilizadas com o advindo da pandemia (home office, audiências virtuais, videoconferências) e também ao enfrentamento das ameaças de segurança mais recentes. Além disso, o firewall atualmente instalado não possui portas de rede de alta velocidade (acima de 10 Gbps), fundamentais em um cenário onde as aplicações do Poder Judiciário estão todas em um processo de migração para a nuvem.

Considerando esse contexto, torna-se imprescindível garantir a confiabilidade e segurança da informação que transitará pela rede do PJES, assim como sua integridade, confidencialidade, autenticidade e disponibilidade no acesso, de forma a garantir a preservação e segurança da informação que, hoje, é considerada um dos ativos mais valiosos, não só pela sua importância estratégica, mas também por ser um elemento de fundamental importância para tomada de decisões pelas instituições e órgãos públicos.

Ademais, é de notório conhecimento que, desde 2020, os ataques cibernéticos tem sido cada vez mais frequentes, principalmente após a pandemia, período no qual houve vários ataques virtuais a órgãos do Poder Judiciário, os quais foram responsáveis pela paralisação das atividades judiciárias de alguns tribunais, promovendo solução de continuidade na prestação dos serviços públicos nessas instâncias.

A resposta do CNJ, emitida na esteira dos eventos de 2020, veio, em primeiro lugar, na forma de recomendações aos órgãos do Poder Judiciário para que concentrassem esforços no sentido de se prepararem para os ataques cibernéticos. Após, foram emitidas várias resoluções (360/2020, 361/2020, 362/2020, 363,2020, 370/2021 396/2021), na qual o CNJ efetivamente determina que os Tribunais promovam ações proativas e paliativas que tenha como objetivo a conformidade das melhores práticas de prevenção, gerenciamento e investigação de ataques cibernéticos no sentido de evitar ou mitigar os danos que tais ataques são capazes de produzir.

Por todo o exposto, a contratação de recursos de segurança da informação por meio de uma solução de firewall, visa dotar a infraestrutura de TIC do PJES de meios tecnológicos efetivos para proteção das aplicações disponibilizadas na modalidade web que, atualmente, perfaz a maior parte das aplicações disponibilizadas pelo TJES, tornando-se absolutamente indispensável a uti

lização da presente solução para garantir a continuidade e efetividade da prestação jurisdicional.

3- DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO:

1. REQUISITOS TÉCNICOS ESPECÍFICOS:

1.1 Requisitos Técnicos

Este item consta no ADENDO III do Termo de Referência.

1.2 Requisitos de Metodologia do Trabalho

A CONTRATADA irá disponibilizar acesso ao sítio de internet da fabricante para que a Seção de Segurança da Informação possa verificar as licenças com suporte, em nome do PJES, em até 30 (trinta) dias após a assinatura do contrato.

A CONTRATADA deverá ter conhecimento e capacitação técnica para prestar os serviços relacionados a este objeto, sendo que tais serviços poderão ser demandados a qualquer tempo por meio de abertura de chamados.

Manter, durante todo o período de vigência do ajuste, todas as condições exigidas para a habilitação.

Disponibilizar recursos humanos qualificados para a execução do serviço e em quantidade suficiente para atender aos chamados abertos.

Fiscalizar regularmente os seus recursos designados para a prestação dos serviços, verificando as condições em que as atividades estão sendo realizadas.

Corrigir todos os serviços que não forem considerados satisfatórios pelo CONTRATANTE, mediante justificativa, sem que caiba qualquer acréscimo no custo contratado, independentemente das penalidades previstas e dos Níveis de Qualidade fixados.

Executar fielmente o objeto contratado, de acordo com as normas legais, em conformidade com a proposta apresentada e com as orientações do PJES, observando sempre os critérios de qualidade.

A CONTRATADA disporá do prazo de 05 (cinco) dias úteis para apresentar justificativas prévias ao CONTRATANTE quanto ao descumprimento do prazo acordado. Sendo aceitas as justificativas, não haverá penalidade à CONTRATADA.

A Ordem de Serviço - OS somente poderá ser encerrada quando todos os objetivos propostos forem plenamente atingidos e os serviços realizados e entregues com a qualidade demandada e devidamente aceitos pelo demandante, aprovada pelo Gestor do Contrato.

Antes do fechamento de cada OS, a CONTRATADA consultará o usuário responsável pela abertura da mesma, que avaliará e aprovará o serviço realizado.

A prestação de serviços, objeto desta contratação, não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração, sendo vedada qualquer relação em que fique configurada a pessoalidade e a subordinação.

O gestor do contrato verificará periodicamente a existência de atualizações e possíveis problemas.

Todas as aberturas de chamados serão realizadas por telefone, portal web ou e-mail, e deverão ser registradas para que se possa ter controle do prazo de resposta e qualidade do serviço.

A Contratada se obriga a fiscalizar regularmente os seus recursos designados para a prestação dos serviços verificando as condições em que as atividades estão sendo realizadas.

1.3 Requisitos de Níveis de Serviço

Os níveis de serviços são critérios objetivos definidos pelo CONTRATANTE e aceitos pela CONTRATADA, compostos por indicadores e metas para avaliação de serviços relativos aos ambientes tecnológicos, mantendo os níveis de disponibilidade e qualidade de serviços necessários às atividades do CONTRATANTE.

A frequência de aferição e ateste dos níveis de serviços será mensal, através da apresentação pela CONTRATADA do relatório mensal, que terá os indicadores verificados pela equipe do CONTRATANTE.

A análise dos níveis de serviço pelo CONTRATANTE poderá resultar em glosas e/ou penalidades, caso a CONTRATADA não cumpra com os seus compromissos de qualidade e desempenho.

Será considerado para efeitos dos níveis exigidos o Prazo de Resolução que é o tempo decorrido entre a abertura do chamado pelo CONTRATANTE e a sua efetiva resolução pela CONTRATADA.

Na abertura do chamado, será definida a categoria de prioridade/severidade (baixa, média, alta e crítica).

- **Alta:** Significa que a solução ficou inoperante ou ocorreu falha de grande impacto que fez com que a solução parasse de funcionar. Para este nível de severidade o encaminhamento do chamado para atendimento deverá ser imediato, com tempo de resposta de resolução máxima de 4 (quatro) horas, a contar da recepção do chamado, sendo preferencialmente prestado na modalidade presencial (on-site). Nestes casos, considerar-se-á como resolução o retorno do funcionamento da solução, seja através de implementação de uma solução definitiva para o incidente, seja por meio de uma solução temporária para colocação emergencial da solução novamente em operação;
- **Média:** Incidentes que causem redução de performance da solução, tais como lentidão intermitente, erros e falhas em determinados módulos ou recursos e falha no funcionamento de políticas já implementadas; Para este nível de severidade o tempo de resposta deverá ser de até 8 (oito) horas, para resolução total ou encontro de solução temporária de contorno;
- **Baixa:** Incidentes de baixo impacto, que não causem falhas ou redução de performance da solução, ou que afetem módulos ou funcionalidades que não sejam consideradas como essenciais para o funcionamento da solução, tais como ferramenta de geração de relatórios, acesso à dashboards, funções administrativas da solução (edição de grupos de administração, por exemplo). Inclui também chamados para esclarecimento de dúvidas sobre a configuração ou funcionamento da solução. Para este nível de severidade o tempo de resposta deverá ser de até 02 (dois) dias úteis, a contar da abertura do chamado.

Abaixo, segue a tabela com o Acordo de Níveis de Serviço referente ao serviço de suporte técnico, com as seguintes severidades e prazos máximos de resolução

Acordo de Serviço	Descrição	Tempo
Severidade Alta	Serviço indisponível e inoperante. Falha de impacto operacional significativo.	Prazo de Resolução: Até 04 (quatro) horas corrida, a contar da abertura do chamado.
Severidade Média	Um ou mais componentes dos equipamentos/software não estão funcionando, todavia, o problema pode ser contornado com impactos operacionais moderados.	Prazo de Resolução: Até 8 (oito) horas, a contar da abertura do chamado.
Severidade Baixa	Informacional. Não causa falha ou redução de performance da solução.	Prazo de Resolução: Até 02 (dois) dias úteis, a contar da abertura do chamado.

INDICADORES DE NÍVEL DE SERVIÇO						
Indicador	**Descrição**	**Severidade**	**Período**	**Forma de Cálculo**	**Medida**	**Meta**
1	Índice de Resolução de Chamados	Alta, Normal e Baixa	Mensal	Total de chamados resolvidos atendidos no prazo estipulado / Total de chamados recebidos x 100	%	95
2	Índice de Disponibilidade	-	Mensal	(Tempo em minutos no mês de referência - Tempo em minutos de indisponibilidade no mês de referência) / Tempo em minutos no mês de referência x 100	%	99,9

1.4 Requisitos de suporte técnico e chamados

O serviço de suporte técnico à solução fornecida e implementada destina-se a:

Manutenção e atualização de softwares que compõem a solução ofertada.

A abertura do chamado será realizada através do Servicedesk do CONTRATANTE. Esse chamado será encaminhado automaticamente para o Grupo de Serviços da CONTRATADA, previamente cadastrado no sistema de atendimento do CONTRATANTE, estando disponível para acesso da CONTRATADA para seu atendimento. Após a abertura do chamado será encaminhado, automaticamente, um email à CONTRATADA, com o número e informações do chamado.

Em caso de indisponibilidade do Servicedesk:

- O atendimento será realizado via telefone gratuito para atendimento de Assistência Técnica, ou por meio de uma central de atendimento para abertura e fechamento de chamados, disponibilizado via sítio eletrônico indicado pela CONTRATADA.
- Neste caso, a CONTRATADA deverá também disponibilizar acesso web ao seu sistema de atendimento, para abertura de chamados técnicos e solicitações de serviços, bem como acompanhamento dos mesmos.

As informações relativas aos chamados deverão ser atualizadas automaticamente sempre que houver alguma alteração em sua situação. O acompanhamento online da resolução de chamados pelo CONTRATANTE deverá ser feito através do sistema de atendimento.
Para cada incidente, será gerado um número de chamado que será usado para controle.

O chamado só será considerado encerrado quando a resolução for validada e fechada pelo 3º (terceiro) Nível de Atendimento do CONTRATANTE (STI), ou seja, a CONTRATADA resolverá o chamado e o 3º (terceiro) Nível de Atendimento do CONTRATANTE (STI), o validará e o encerrará.

Não haverá limite de quantidade de chamados remotos durante a vigência do contrato.

Na abertura do chamado será definida a categoria de prioridade (baixa, normal e alta).

A CONTRATADA deverá informar o número do chamado e disponibilizar um meio de acompanhamento do seu estado.

Ao final de cada atendimento, a CONTRATADA deverá emitir relatório técnico contendo as seguintes informações: número do chamado, categoria de prioridade, descrição do problema e da solução, procedimentos realizados, data e hora da abertura e do fechamento do chamado, data e hora do início e do término da execução dos serviços, identificação do técnico da empresa.

A CONTRATADA deverá prestar o serviço de suporte técnico durante toda a vigência do contrato para:

- Resolução de incidentes;
- Resolução de problemas;
- Esclarecimento de dúvida sobre configuração e utilização da solução.

Todos os custos diretos, indiretos, trabalhistas, deslocamentos, hora técnica, alimentação, entre outros, que fazem parte do escopo deste atendimento, são de responsabilidade da CONTRATADA.

A CONTRATADA deverá prestar suporte técnico durante toda a vigência do contrato conforme requisitos deste documento.

O serviço de suporte técnico deverá ser prestado pela CONTRATADA ou pelo FABRICANTE da solução.

1.5 Requisitos de garantia e manutenção

Grupo Único - Solução de segurança de rede com Firewall de última geração (NGFW)

A garantia dos equipamentos deverá ser oficial do fabricante dos equipamentos, sem prejuízo à responsabilidade integral da CONTRATADA quanto aos atendimentos dos níveis de serviço.

Os serviços de Garantia, Suporte Técnico e Manutenção DEVEM ESTAR INCLUSOS NO VALOR TOTAL DA PROPOSTA.

Entende-se por serviços de “Garantia”, “Suporte” e “Manutenção”, doravante denominados unicamente como “Garantia”, toda atividade do tipo corretiva não periódica que variavelmente poderá ocorrer, durante todo o período de garantia. Ela possui suas causas em falhas e erros no Software/Hardware e trata da correção dos problemas atuais e não iminentes de fabricação destes. Esta “Garantia” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados pela presente solução.

Os equipamentos e softwares adquiridos nesse processo deverão possuir garantia do fabricante ou de empresa autorizada pelo fabricante para prestação deste serviço no Brasil, com prazo mínimo de duração de 60 (sessenta) meses, contados a partir do recebimento definitivo da solução, que se dará somente quando de sua completa instalação, configuração e início de operação;

Durante todo o prazo de vigência a garantia deverá incluir os serviços de manutenção preventiva e corretiva, cuja periodicidade de execução deverá se dar de acordo com a solicitação e necessidades do CONTRATANTE, bem como por meio de recomendações técnicas da fabricante da solução;

A CONTRATADA e/ou o fabricante da solução deverá dispor de assistência técnica especializada para investigar, diagnosticar e resolver incidentes e problemas relativos aos produtos fornecidos.

Os serviços de garantia, assistência técnica e suporte técnico deverão ser prestados 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, no local onde os equipamentos se encontrarem instalados (on-site), por técnicos devidamente habilitados e credenciados pela fabricante, com nível de certificação compatível com as atividades a serem executadas, e sem qualquer ônus adicional.

Quaisquer peças, componentes ou outros materiais que substituírem os defeituosos deverão ser originais do fabricante, sem uso anterior e de qualidade e características técnicas iguais ou superiores aos existentes no equipamento, sem qualquer ônus adicional.

A manutenção preventiva deverá, no mínimo, incluir:

Atualização de todos os componentes de software da solução, incluindo patches de segurança, firmwares e versões de sistema operacional, seja para corrigir problemas identificados, seja para implementação de melhorias e acesso a novas funcionalidades;

Acesso e atualização de assinaturas de proteção, assim como às bases de dados mantidas pela fabricante, necessárias para o correto e pleno funcionamento da solução, tais como Black e White Lists, assinaturas do tipo “Zero Day”, lista de aplicativos confiáveis, etc;

A manutenção corretiva deverá, no mínimo, incluir:

Reposição de peças, componentes e equipamentos que apresentarem defeito ou falha de funcionamento, abrangendo todos os itens que compõem a solução, incluindo seus acessórios, módulos de expansão, transceivers ou outros equipamentos fornecidos pela CONTRATADA para funcionamento da solução;

Em caso de defeitos de fabricação ou a necessidade de substituição hardware, a garantia deverá incluir envio de peças ou equipamentos de reposição nos locais especificados pelo CONTRATANTE. O envio da peça ou equipamento de reposição deverá ser realizado, no máximo, até o fim do próximo dia útil após a detecção da falha;

1.6 Requisitos Temporais:

Os prazos para execução do objeto da contratação estão estabelecidos na tabela abaixo:

ETAPA	Eventos	Prazos
ETAPA 1	Prestação de Garantia Contratual	10 dias corridos após a convocação para esse fim
ETAPA 2	Assinatura do Contrato	5 (cinco) dias úteis após a convocação para esse fim
ETAPA 3	Reunião de "kick-off"; - Reuniões para levantamento de requisitos; - Levantamento das configurações atuais; - Monitoramento do ambiente. Entrega do Projeto de Instalação Física da Solução	20 (vinte) dias úteis a partir da ETAPA 2
ETAPA 4	- Instalação física da solução; - Elaboração da configuração lógica.	40 (quarenta) dias úteis a partir da ETAPA 3
ETAPA 5	- Implantação das configurações no firewall, IPS, etc.	20 (vinte) dias úteis a partir da ETAPA 4
ETAPA 6	- Levantamento requisitos - Monitoramento - Coleta das configurações - Elaboração das configurações -Operação assistida - Migração firewall	30 (trinta) dias corridos a partir da ETAPA 5
ETAPA 7	- Migração de unidade piloto - Resolução de problemas - Ajustes necessários	10 (dez) dias úteis a partir da ETAPA 6
ETAPA 8	- Migração de segunda unidade piloto (área) - Resolução de problemas - Ajustes necessários	10 (dez) dias úteis a partir da ETAPA 7
ETAPA 9	- Migração de todo o parque - Resolução de problemas - Ajustes necessários	10 (dez) dias úteis a partir da ETAPA 8
ETAPA 10	- Operação assistida - Repasse de conhecimento	60 (sessenta) dias corridos a partir da ETAPA 9
ETAPA 11	Treinamento	Data a ser definida pelo Contratante de acordo com a emissão da ordem de serviço

1.7 Requisitos de Implantação

Cronograma das atividades:

ETAPA	ATIVIDADES	PRAZO	RESPONSÁVEL(IS)	ENTREGA(S) PRINCIPAL(IS)
ETAPA 1	- Reunião de "kick-off"; - Reuniões para levantamento de requisitos; - Levantamento das configurações atuais; - Monitoramento do ambiente.	20 (vinte) dias úteis	CONTRATADA	Projeto de instalação Física
ETAPA 2	- Instalação física da solução; - Elaboração da configuração lógica.	40 (quarenta) dias úteis	CONTRATADA	- Equipamento instalado fisicamente. - Projeto de configuração Lógico - Inventário dos equipamentos.
ETAPA 3	- Implantação das configurações no firewall, IPS, etc.	20 (vinte) dias úteis	CONTRATADA	- Apresentação das configurações; - ATA de Reunião para agendamento da migração do firewall.
ETAPA 4 (Filtro URL)	- Levantamento requisitos - Monitoramento - Coleta das configurações - Elaboração das configurações -Operação assistida - Migração firewall	30 (trinta) dias corridos	CONTRATADA	- Apresentação das configurações - Aceite da migração do firewall
ETAPA 5	- Migração de unidade piloto - Resolução de problemas - Ajustes necessários	10 (dez) dias úteis		- Aceite da unidade piloto
ETAPA 6	- Migração de segunda unidade piloto (área) - Resolução de problemas - Ajustes necessários	10 (dez) dias úteis		- Aceite desta segunda unidade piloto
ETAPA 7	- Migração de todo o parque - Resolução de problemas - Ajustes necessários	10 (dez) dias úteis		- Aceite da migração pela equipe de Segurança da Informação da STI.
ETAPA 8	- Operação assistida - Repasse de conhecimentos	60 (sessenta) dias corridos		- Aceite final

1.8 Detalhamento das atividades/procedimentos e entregas

Etapa 01

- Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;
- Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos servidores e aos usuários externos.
- O PJES irá disponibilizar, para instalação do equipamento, os seguintes itens de configuração e serviços de apoio:
    - Espaço em um rack de equipamentos padrão 19" suficiente para os appliances NGFW e para organização dos cabos de rede;
    - Tomadas de energia padrão 3 pinos (NBR 14.136) em quantidade suficiente para energizar toda a solução de maneira adequada;
    - Portas Gigabit Ethernet e SFP/SFP+ para interconexão das interfaces de rede dos Firewalls NGFW e os switches de rede do PJES;
    - Alocação de endereços IP e ranges de sub-rede, conforme orientação a ser repassada pela equipe técnica da contratada (pré-requisitos);
- **Entregas da Etapa 01**

O Projeto de instalação física deve conter, no mínimo, os seguintes itens:

- **Levantamento de Requisitos:**
    - Identificação dos requisitos específicos de segurança.
    - Determinação das necessidades de largura de banda.
    - Avaliação das políticas de segurança da empresa.
- **Seleção do Firewall:**
- Escolha do modelo de firewall adequado com base nos requisitos.
- Consideração das funcionalidades necessárias (inspeção profunda de pacotes, VPN, etc.).
- Avaliação da capacidade de throughput do firewall.
- **Localização Física:**
- Identificação do local ideal para a instalação do firewall (por exemplo, sala de equipamentos, data center).
- Garantia de que o local escolhido seja seguro, acessível e esteja de acordo com os requisitos ambientais.
- **Requisitos de Energia:**
- Garantia de fonte de energia estável e ininterrupta.
- Consideração de equipamentos como no-breaks ou geradores de energia.
- **Requisitos de Refrigeração:**
- Avaliação da necessidade de refrigeração adicional, dependendo do ambiente.
- Garantia de fluxo de ar adequado para resfriamento do equipamento.
- **Conectividade de Rede:**
- Configuração de interfaces de rede no firewall.
- Planejamento e implementação de VLANs, se aplicável.
- Integração com switches e roteadores existentes.
- **Configuração Física:**
- Instalação física do firewall no rack.
- Conexão de cabos de alimentação e de rede.
- Configuração de interfaces físicas.
- **Documentação:**
- Criação de documentação detalhada sobre a configuração física do firewall.
- Inclusão de informações sobre políticas de segurança e procedimentos operacionais.

Etapa 02

- **Inventário dos componentes dos dois appliances:**
    - Entende-se por inventário dos appliances o processo de verificação física dos equipamentos e dos acessórios entregues e se os mesmos estão de acordo com as especificações técnicas exigidas no Termo de Referência. Este processo será realizado por um servidor da STI, que fará todas as conferências necessárias para aceitar a entrega dos equipamentos para que se possa proceder com a instalação física.
- **Instalação física:**
    - Esta etapa deverá incluir a integração de todas as peças, componentes e acessórios necessários para seu funcionamento, a colocação dos equipamentos na rack padrão 19” disponibilizada pela STI, e a conexão física de todos os cabos (power cords, fibre channel e UTP), incluindo a instalação e ativação de transceivers e a interconexão de suas interfaces com as interfaces de rede dos switches do PJES e das operadoras de link de dados.
    - Após a instalação física deve-se efetuar a ligação inicial do equipamento e realizar todos os testes de verificação e de diagnóstico solicitados pelo manual do fabricante, com o objetivo de verificar se todos os componentes estão em perfeito funcionamento.
- **Entregáveis da Etapa 02:**
    - Aceite do equipamento após inventário;
    - Instalação física do equipamento concluída;
    - Documento de configuração lógica da solução, que deverá conter, no mínimo, os seguintes itens;
        - **Definição de Objetivos e Requisitos**
            - Identificação dos objetivos de segurança.
            - Levantamento de requisitos específicos, como controle de acesso, VPN, inspeção de pacotes, etc.
        - **Políticas de Segurança**
            - Desenvolvimento de políticas de segurança claras.
            - Especificação das regras para tráfego permitido e bloqueado.
            - Definição de políticas de NAT (Network Address Translation) se necessário.
        - **Segmentação de Rede:**

        - Criação de zonas de segurança e segmentação de rede.
        - Implementação de VLANs e políticas de comunicação entre zonas.
    - **Controle de Acesso**
        - Configuração de regras de controle de acesso para permitir ou negar o tráfego com base em endereços IP, portas, protocolos, etc.
        - Implementação de regras baseadas em políticas específicas.
    - **Inspeção Profunda de Pacotes**
        - Ativação de recursos de inspeção profunda de pacotes para análise detalhada do tráfego.
        - Configuração de regras para detectar e bloquear ameaças específicas.
    - **VPN (Virtual Private Network)**
        - Configuração de túneis VPN para acesso de usuários externos..
        - Definição de políticas de VPN para criptografia e autenticação.
    - **Políticas de Logging e Auditoria**
        - Configuração de logs para registrar eventos de segurança.
        - Definição de políticas de auditoria para monitorar atividades suspeitas.
    - **Atualizações e Patches**
        - Planejamento para aplicação regular de atualizações e patches de segurança.
        - Configuração de políticas para gerenciamento de versões de firmware.
    - **Balanceamento de Carga**
        - Implementação de balanceamento de carga, se necessário.
        - Distribuição equitativa do tráfego entre diferentes servidores.
    - **Configuração de Recursos Avançados**
        - Ativação de recursos avançados, como prevenção de intrusões (IPS), anti-vírus integrado, filtragem de conteúdo, etc.
        - Ajustes finos para otimizar o desempenho e a segurança.
    - **Contingências e Planos de Recuperação**
        - Desenvolvimento de planos de contingência para lidar com situações de falha ou ataque.
        - Configuração de políticas de backup e recuperação.
    - **Documentação Detalhada**
        - Criação de documentação abrangente para a configuração do firewall.
        - Inclusão de informações sobre políticas, endereçamento IP, diagramas de rede, etc.

ETAPA 03

- **Configuração inicial:**
    - **Com o equipamento devidamente ligado e com seus componentes integralmente funcionais, deve-se realizar a configuração inicial da solução, de acordo com as recomendações estabelecidas pelo fabricante, incluindo atividades como:**
        - Atribuição de endereço(s) IP(s) para gerenciamento remoto;
        - Configuração de hostnames e integração à rede interna;
        - Configuração de data e hora e timezone;
        - Cadastramento dos usuários gerenciadores do equipamento;
        - Instalação e atualização do sistema operacional da solução, se necessário;
        - Atualização de drivers, firmwares e outros softwares acessórios necessários para o pleno funcionamento do equipamento;
        - Ativação de recursos básicos para início da configuração avançada da solução, incluindo licenças de software;
        - Ativação da console de gerenciamento remoto da solução.
- **Configuração avançada:**

Com a configuração inicial concluída, deverá ser realizada a configuração avançada da solução, com o objetivo de torná-lo apto a executar as funções de segurança de redes, incluindo obrigatoriamente:

- Configuração da solução para monitoramento dos links de dados, de modo a realizar o roteamento de tráfego caso o link operacional deixe de funcionar (falha no tráfego em rotas ou em interfaces);
- Configuração de políticas de segurança para melhor controle do tráfego entre as redes internas do PJES e entre a sua rede interna e a rede externa (internet), utilizando-se dos recursos avançados de um Firewall NGFW, como controle de aplicações e controle por identificação de usuários;
- Configurar a nova solução para que não sobreponha ou inabilite os recursos de segurança já presentes e operacionais no ambiente do PJES, como o antivírus/antimalware Broadcom SEP 14;
- Ativação e calibragem das regras de monitoramento de tráfego, alertas, notificações, logging e auditoria;

- Configuração do firewall com todas as funcionalidades da solução atual, minimamente configuradas na nova solução de Firewall-NG.
- **Testes e homologação:**
- Etapa a ser realizada em conjunto com a equipe técnica da STI, onde será realizada a validação das regras e configurações implementadas;
- Os testes devem abranger todos os módulos ativados da solução, incluindo no mínimo as seguintes funcionalidades e recursos do ambiente:
    - Controle de tráfego intrazonas;
    - Controle de tráfego entre zonas distintas;
- Teste de execução de backup e restore de dados da rede interna via Veritas NetBackup, comprovando que a solução continua apta a realizar os procedimentos de backup e restore do ambiente;
- Testes de envio e recebimento de e-mails por meio da solução GMail;
- Teste de comunicação entre os componentes Google Workspace;
- Teste de comunicação das soluções de container presentes no ambiente PJES: Docker e AWS ECS, em especial a comunicação das aplicações e do orquestrador com os demais hosts da rede interna do PJES e com o proxy reverso;
- Teste de execução de rotinas de extração e transformação de dados (ETL/Data Warehouse) no SQL Server, incluindo sua comunicação com os servidores de geração de dashboards e relatórios (Power BI);
- Teste de comunicação das ferramentas de monitoramento de ambiente – Zabbix e Grafana;
- Teste de conexão via VPN client-to-site, com utilização de pelo menos um usuário para cada perfil de acesso VPN configurado;
- Teste de validação das regras de QoS configuradas;
- Coleta e extração de dados de auditoria da solução de segurança de rede: Geração de relatórios ou dashboards, filtragem de informações e logging.
- **Entregáveis da Etapa 03**
- Verificação da configuração do firewall, com todas as funcionalidades da solução atual, minimamente configuradas na nova solução de Firewall-NG.
- Documentação dos resultados das configurações básicas e avançadas efetuadas e dos testes de homologação.
- Aceite da documentação apresentada.
- Ata de reunião de agendamento para migração do equipamento.

ETAPA 04

- Migração da solução atual de filtro de conteúdo web Skyhigh Secure Webgateway para a solução de filtro de URL a ser ofertada dentro da solução Firewall NGFW, respeitando as regras de perfil de acesso estabelecidas atualmente por meio da Política de Acesso à Internet do PJES, Ato nº 42/2018;
- Validação mínima dos 3 perfis de acesso previstos pelas normas internas de segurança do PJES, além de teste de acesso à internet sem nenhum filtro aplicado;
- Personalização da página de bloqueio;
- Validação do tráfego das principais aplicações do PJES: Comunicação entre múltiplas camadas das aplicações principais do PJES, verificando se seus componentes estão processando os dados corretamente. Deve-se, obrigatoriamente, testar a comunicação entre as camadas de apresentação, de regras de negócio, persistência em bases de dados e autenticação externa de usuários;
- **Entregáveis da Etapa 04**
- Documentação das configurações e testes realizados no Filtro Web.
- Aceite do documento.
- Aceite da migração do equipamento.

ETAPA 05

- Direcionar o tráfego de rede da unidade-piloto para a nova solução de NGFW;
- Verificar eventuais problemas e corrigi-los;
- Executar os ajustes que se fizerem pertinentes.
- **Entregáveis da Etapa 05**
- Aceite da unidade-piloto.

ETAPA 06

- Direcionar o tráfego de rede da segunda unidade-piloto para a nova solução de NGFW;
- Verificar eventuais problemas e corrigi-los;
- Executar os ajustes que se fizerem pertinentes.
- **Entregáveis da Etapa 06**
- Aceite da segunda unidade-piloto.

ETAPA 07

- Direcionar o tráfego de rede de todo o PJES para a nova solução de NGFW;
- Verificar eventuais problemas e corrigi-los;
- Executar os ajustes que se fizerem pertinentes.

- **Entregáveis da Etapa 07**
- Aceite da migração do equipamento pela equipe de Segurança da Informação da STI.

ETAPA 08

- Operação assistida.
- Repasse de conhecimentos.
- **Entregáveis da Etapa 08**
- **Documentação Final**
    - O processo de implantação deverá ser devidamente documentado pela CONTRATADA ao longo de todo o período de execução. Ao fim do processo a CONTRATADA deverá apresentar um relatório com o detalhamento da implantação, contendo todas as etapas, histórico de mudanças, diagramas e detalhamento da estrutura da solução, procedimentos adotados, configurações efetuadas e resultado dos testes e homologação;
    - A entrega deste relatório é obrigatória, sendo este o principal artefato comprobatório de conclusão da execução do serviço, a ser utilizado pela equipe técnica de contratação para validação do serviço e emissão do Termo de Recebi**mento Definitivo da solução.**
- **Relatório detalhado de todo o processo de implantação.**
- **Aceite definitivo da migração da solução.**
- **Acompanhamento pós-migração.**

Após cada fase, a CONTRATANTE validará os entregáveis. Havendo não conformidade dos entregáveis, fica estabelecido o prazo de 5 dias úteis para ajustes, contados a partir da data de notificação. Após este prazo, restando inconformidades, será aplicada penalidade (multa)

As fases são sequenciais e a contagem dos prazos de cada fase, se dará no dia seguinte à aprovação do(s) entregáveis da fase anterior.

1.9 Requisitos Legais

A presente contratação tem como referência os seguintes instrumentos legais: Constituição Federal de 1988; Lei nº 14.133/2021; Resolução nº 468/2022 do CNJ; Instrução Normativa nº 94/2022 do ME; e demais instrumentos correlatos.

1.10 Requisitos de Segurança da Informação

São requisitos exigidos com relação à Política de Segurança da Informação, na forma da Resolução nº 06/2018, do Ato Normativo nº 41/2018 e do Ato Normativo nº 42/2018, todos deste PJES, devendo a CONTRATADA:

- À Política de Segurança adotada pelo PJES e as configurações de hardware e de softwares decorrentes;
- Ao processo de instalação, configuração e adaptações de produtos, ferramentas e equipamentos;
- Ao processo de implementação, no ambiente do PJES, dos mecanismos de criptografia e autenticação.
- Obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pelo PJES.

Executar todos os testes de segurança necessários e definidos nas legislações pertinentes, bem como executar seus trabalhos dentro das diretrizes ali estabelecidas.

Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse do PJES ou de terceiros de que tomar conhecimento em razão da execução do objeto do Contrato, devendo orientar seus empregados nesse sentido.

Responsabilizar-se pelos materiais, produtos, ferramentas, instrumentos e equipamentos eventualmente disponibilizados para a execução dos serviços, não cabendo ao PJES qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer, cabendo à CONTRATADA o seu ressarcimento, em quantidade e qualidade, sem prejuízo das penalidades cabíveis.

Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do PJE.

Manter em caráter confidencial, mesmo após o término do prazo de vigência ou de rescisão do Contrato, as informações relativas:

- À Política de Segurança adotada pelo PJES e as configurações de hardware e de softwares decorrentes;
- Ao processo de instalação, configuração e adaptações de produtos, ferramentas e equipamentos;
- Ao processo de implementação, no ambiente do PJES, dos mecanismos de criptografia e autenticação.

1.11 Requisitos de Segurança Institucional

CONTRATADA deve zelar pelo cumprimento da Resolução nº 031/2018 do PJES, dando ciência do seu conteúdo a todos os seus respectivos agentes.

CONTRATANTE deverá cientificar a CONTRATADA sobre as normas internas vigentes relativas à segurança, inclusive aquelas relacionadas ao controle de acesso de pessoas e veículos, bem como sobre a Política de Segurança da Informação.
Para que a CONTRATADA atenda aos requisitos exigidos com relação à Política de Controle de Acesso, deverá:

Responsabilizar-se pelo credenciamento e descredenciamento de acesso às dependências do PJES, assumindo quaisquer prejuízos porventura causados por dolo ou culpa de seus profissionais.

Solicitar, por escrito, credenciamento e autorização de acesso para os recursos da CONTRATADA.

Informar e solicitar ao GESTOR ou FISCAL TÉCNICO do contrato, no prazo máximo de 24 (vinte e quatro) horas, o descredenciamento dos recursos desvinculados da prestação de serviços com o PJES.

Devolver para o CONTRATANTE todos os recursos e equipamentos eventualmente disponibilizados, como crachás, cartões certificadores, “pendrives” e outros, de propriedade do PJES, juntamente com a solicitação de descredenciamento.

1.12 Requisitos sociais, ambientais e culturais

A CONTRATADA deverá orientar sua equipe técnica sobre as boas práticas voltadas ao consumo consciente, redução de desperdício dos recursos naturais e coleta seletiva, inclusive à adequada destinação dos resíduos porventura gerados na execução do contrato, com o objetivo de contribuir para a preservação do meio ambiente, quando aplicável.

A presente Contratação também visa a:

- Alcançar melhoria sociocultural no relacionamento dos usuários com os recursos tecnológicos atuais, meios de comunicação e maior transparência nas atividades desenvolvidas pelo PJES:

- Possibilitar a modernização do PJES para um melhor atendimento jurisdicional com agilidade, eficiência e eficácia;Prover maior celeridade na administração das demandas apresentadas ao PJES, assim como a diminuição dos custos dos serviços prestados.

1.13 Requisitos de qualificação técnica da contratada

A LICITANTE melhor classificada deverá comprovar capacitação técnica por meio de:

Da empresa:

A CONTRATADA deverá apresentar, no mínimo, 01 (um) Atestado(s) de Capacidade Técnica (ACT), emitidos por outras empresas, públicas ou privadas, com identificação do emitente (nome completo, e-mail e telefone de contato), com características técnicas, prazos compatíveis e complexidade similares ao objeto especificado no Termo de Referência, informando o período e o local da prestação dos serviços de suporte / orientação técnica / capacitação técnica. Caso seja necessário, a CONTRATADA poderá apresentar mais de um atestado, a fim de comprovar a capacidade.

Deverá haver comprovação de experiência mínima de 3 (três) anos na prestação dos serviços, permitindo o somatório de atestados de diferentes períodos, sem a necessidade de continuidade ininterrupta.

O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

A CONTRATADA terá o prazo de 10 (dez) dias corridos a partir da assinatura do contrato, para apresentação dos documentos comprobatórios da qualificação técnica do instrutor.

Para aprovação do profissional da CONTRATADA, por parte do CONTRATANTE, a mesma deverá apresentar o currículo e outros documentos que comprovem o seu perfil.

O CONTRATANTE terá um prazo de até 05 (cinco) dias corridos para validar as documentações apresentadas, podendo solicitar a substituição do profissional que não atenda ao perfil mínimo indicado.

Nos casos em que seja necessária a substituição, pela CONTRATADA, do profissional, a empresa deverá assegurar que o novo profissional detenha perfil igual ao especificado neste documento.

Do Instrutor especialista na solução:

Nível Superior completo na área de Tecnologia da Informação ou nível superior completo em outra área com especialização na área Tecnologia da Informação, com carga horária mínima de 360 (trezentas e sessenta) horas;

Para a capacitação da solução, o instrutor deverá apresentar experiência de treinamentos anteriores na solução.

1.14 Requisitos de treinamento

Treinamento oficial sobre a solução de Firewall NGFW oferecida no Grupo Único deste Termo de Referência, a ser ministrada a servidores da Seção de Segurança da Informação e Telecomunicações, que atuarão diretamente na administração e operação da solução após sua implementação;

Treinamento oficial do fabricante com repasse de conhecimento específico sobre a solução instalada para, no mínimo, 08 (oito) servidores da Seção de Segurança da Informação e Telecomunicações;

Duração mínima: 5 (cinco) dias ou 30 (trinta) horas semanais, a depender da modalidade de execução do treinamento, com duração diária máxima de 6 (seis) horas;

O Contratante deverá apresentar uma grade com os próximos treinamentos, limitados a seis meses posteriores, com datas, horários, modalidades e localidade, para agendamento dos servidores nas turmas. A grade de cursos deverá disponibilizar cursos na modalidade presencial e remota, sendo a escolha a critério do servidor.

O treinamento deverá ser ministrado em horário comercial, e deverá ser realizado pelo fabricante ou por uma empresa parceira devidamente certificada e autorizada pelo fabricante a ministrar treinamentos oficiais;

Modalidade: Preferencialmente na modalidade presencial, nas instalações do fabricante ou do parceiro autorizado, podendo também ser realizada na modalidade remota.

O treinamento deverá oferecer material didático de apoio gratuito aos participantes, seja por meio de mídia física (livros, apostilas, etc.) ou digital (PDF). O material deverá ser cedido individualmente a cada participante, de modo que ele possa levar consigo e consultá-lo posteriormente;

Eventuais despesas de deslocamento, hospedagem e alimentação dos instrutores do curso serão de responsabilidade integral da CONTRATADA. Já as eventuais despesas de deslocamento, hospedagem e alimentação dos participantes do curso serão de responsabilidade integral da CONTRATANTE;

O treinamento deverá abranger tanto teoria quanto exercícios práticos, voltados para conhecimento da arquitetura da solução, sua implantação, configuração e gerenciamento, além de tratamento de problemas típicos envolvendo a operação da solução

O escopo básico do treinamento deverá conter:

- Arquitetura da solução;
- Configurações iniciais básicas;
- Alta disponibilidade;
- Controle de acesso dos administradores da solução;
- Configuração de Interfaces;
- Configuração dos recursos de Firewall, IPS, Antimalware, Antibot, SSL/TLS Inspection;
- Configuração de realização de backups;
- Testes e realização de restore;
- Aplicação de Patches e Rollback;
- Atualização de versão de todos os componentes da solução ofertada;
- Criação e gerenciamento de Zonas de Segurança, Políticas de Segurança e Endereçamento NAT;
- Controle por Identificação de Aplicações;
- Controle por Identificação de Usuários, com conexão a fontes externas de autenticação;

- Criação e gerenciamento de Filtro URL;
- Descriptografia de tráfego;
- Configurações de VPN (SSL e IPSec);
- Monitoramento e Relatórios;
- Logging e Auditoria;
- Configuração de roteamento estático e dinâmico (BGP).

Ao final do treinamento, deverá ser emitido certificado comprobatório da participação de cada servidor da STI. A apresentação destes certificados é requisito obrigatório para a comprovação da execução do serviço, sendo o principal artefato a ser utilizado pela equipe técnica de contratação para validação do serviço e emissão do Termo de Recebimento Definitivo da solução.

O certificado deve conter, no mínimo, as seguintes informações:

- Carga horária;
- Conteúdo programático;
- Data de início e fim do treinamento.

1.15 Requisitos necessários ao atendimento da necessidade

Para o atendimento das necessidades elencadas propõe-se que seja realizada licitação na modalidade Pregão eletrônico, e que a proposta da licitante contenha todos os requisitos necessários ao atendimento da demanda, quantitativos, forma, capacidade técnica da licitante/contratada e demais condições a serem adotadas para a contratação.

O objeto é enquadrado, conforme definição legal, como bem comum, já que possui padrões de desempenho e de qualidade objetivamente definidos em edital, utilizando-se de especificações usuais no mercado. Assim, dever-se-ão observar as disposições trazidas pela Lei n° 14.133/2021 e demais normas correlatas.

- A adjudicação será realizada a uma única empresa, já que o objeto é uno e indivisível. Composto por 1 item: Contratação de sistema unificado de proteção de borda (Firewall), incluindo transferência de conhecimento, serviços de monitoramento, suporte, instalação, implantação, garantia e treinamento para o PJES.

2 DURAÇÃO DO CONTRATO

O sistema unificado de proteção de borda monitora, controla e provê o acesso à rede externa, ou auditoria, requer maturidade, seja, à Internet, para os servidores do PJES e provê (acesso aos sistemas jurídicos disponibilizados pelos TJES para todos os usuários do PJES, além de interligar todas as comarcas. Esse sistema é considerado de missão crítica para a infraestrutura de TI, não somente porque provê infraestrutura para comunicação, mas principalmente devido à segurança proporcionada, que permite uma melhor gestão, maior controle dos acessos, monitoramento e auditoria.

Todas essas configurações serão realizadas e refinadas durante a gestão do contrato, pois se trata de um serviço evolutivo que se adapta ao ambiente do Poder Judiciário, ou seja, é um projeto que requer maturidade.

Assim, visando ter um melhor aproveitamento da solução, além de economicidade e eficiência, objetivando também alcançar a maturidade e manter um serviço de missão crítica operativo e atualizado, optamos para uma contratação de 60 (sessenta) meses, observado o Art. 107 da Lei nº 14.133, de 1º de abril de 2021.

3 REAJUSTAMENTO DE PREÇO

Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado pela administração.

Após o interregno de um ano contado da data do orçamento estimado pela administração, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, na forma do art. 24 da Instrução Normativa nº 01/2019.

Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

4 GARANTIA CONTRATUAL

Será exigida garantia, na forma do art. 96 da Lei nº 14.133/2021, devendo ser prestada junto à Secretaria de Finanças e Execução Orçamentária do CONTRATANTE, dentre as modalidades definidas em citado artigo, no valor equivalente a 5% (cinco por cento) do valor total inicial do contrato, informando a modalidade escolhida, no prazo máximo de 10 (dez) dias corridos, após o recebimento de notificação para tal fim, o que ocorrerá antes da assinatura do contrato.

Caso a pretensa contratada opte pela modalidade de seguro-garantia, o prazo para sua prestação será de 1 (um) mês contado da data de homologação da licitação, na forma do art. 96, § 1º, II, da Lei nº 14.133/2021.

O prazo para a prestação da garantia poderá ser prorrogado, a critério do CONTRATANTE.

A vigência final da apólice deverá se estender pelo prazo mínimo de 30 (trinta) dias contado do encerramento do contrato.

5 NECESSIDADE DE TRANSIÇÃO CONTRATUAL COM TRANSFERÊNCIA DE CONHECIMENTO, TECNOLOGIA E TÉCNICAS EMPREGADAS

A contratada deverá fornecer a documentação de toda a implantação (planejamento, cronograma, melhores práticas, patchs e "as built") e caberá a equipe de segurança da informação manter toda a documentação atualizada, com as definições de configuração e de mudança, pois este item é um requisito da Política de Segurança da Informação. Essa Documentação poderá ser utilizada como um case, no caso de uma nova contratação.

Após o recebimento definitivo da solução pelo PJ/ES,a CONTRATADA fará a operação assistida por 60 (sessenta) dias. Durante este período a solução deverá ser adequada às demandas que surgirem e deverá ocorrer a transferência final de conhecimento.

O perfil do usuário de implantação deverá ser removido, assim como qualquer material não contratado.

5.1 Direitos de propriedade intelectual

Não se aplica uma vez que o código-fonte é de propriedade da fabricante do software.

6 DETALHAMENTO DOS BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO

LOTE ÚNICO	
ITEM	**Descrição**

1	**Solução integrada de proteção de rede do tipo “Next Generation Firewall” (NGFW), incluindo fornecimento de licença, transferência de conhecimento, suporte e garantia.**
2	**Suporte Técnico**
3	**Implantação e Instalação**
4	**Treinamento Firewall NGFW**

4- LEVANTAMENTO DO MERCADO:

1. SOLUÇÕES DISPONÍVEIS:

SOLUÇÃO 01: Renovação dos serviços de suporte e manutenção para a solução já existente no Tribunal de Justiça

A sua utilização, poder de processamento e soluções de defesa e segurança encontram-se, atualmente, deficientes em relação aos atuais Next-Generation Firewall (NGFW). Ademais, a solução atual está no limite dos equipamentos físicos, operando no limite da sua interface de 1 GB. Concentra-se apenas na manutenção do hardware existente, não implicando em melhorias na disponibilidade de rede e segurança de dados institucionais.

SOLUÇÃO 02: Solução no Portal de Software Público Brasileiro

Não existe um único produto baseado em software livre que seja capaz de oferecer todas as funcionalidades oferecidas por outros softwares proprietários reunidas em um único produto. Para implementação da solução por meio de software livre, seria necessário utilizar várias soluções diferentes e não integradas, tais como Firewall Iptables, Web Filter Squid, OpenVPN e IPS Snort etc., aumentando exponencialmente o esforço de implementação e sustentação, falta de garantia em caso de falhas no software e ausência de suporte. Além disso, deve ser considerada a necessidade de capacitação e especialização do corpo técnico existente nas diversas soluções open sources disponibilizadas, sendo incompatível com o quadro de pessoal da área de TIC do PJES, que é insuficiente para atuar como equipe dedicada.

SOLUÇÃO 03: Aquisição de uma nova solução, serviços de implantação, suporte, garantia e capacitação

Prevê a aquisição de uma nova solução de Next Generation Firewall (NGFW), que prevê novas funcionalidades e maior poder de processamento em relação ao atual equipamento, como a proteção de informação perimetral e de rede interna, que inclui stateful firewall com capacidade para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL, criptografia de email, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Algumas dessas funcionalidades, que agregam uma maior proteção aos ativos de informação da Instituição, não são contempladas, atualmente, pela solução de firewall existente no PJES. Essa nova solução proporcionará maior robustez à segurança da rede e do gerenciamento das conexões estabelecidas, garantindo uma maior disponibilidade dos equipamentos.

Solução 04: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs. Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno, sendo, portanto, inviável para utilização por este PJES.

1.1 **Identificação de Soluções**

Disponibilidade de solução de TIC similar em outro órgão ou entidade da Administração Pública:

Conforme item 7 "Estimativa do Valor da Contratação".

Soluções existentes no Portal do Software Público Brasileiro (http://www. softwarepublico.gov.br):

Não aplicável ao objeto almejado.

Capacidade e alternativas do mercado de TIC, inclusive a existência de software livre ou software público:

Não aplicável ao objeto almejado.

Observância às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário;

Não aplicável ao objeto almejado.

Aderência às regulamentações da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil), quando houver necessidade de utilização de certificação digital, observada a legislação sobre o assunto;

Não aplicável ao objeto almejado.

Observância às orientações, premissas e especificações técnicas e funcionais definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus);

Não aplicável ao objeto almejado.

5- DESCRIÇÃO DA SOLUÇÃO COMO UM TODO :

Prevê a contratação de sistema unificado de proteção de borda (Firewall), incluindo fornecimento de licença, transferência de conhecimento, suporte, instalação, implantação, garantia e treinamento para o PJES.

6- ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS

Trata-se de contratação de sistema unificado de proteção de borda (Firewall), que contemple 12 (doze mil) usuários, sendo:

- 7.000 (sete mil) usuários internos
- 3.000 (três mil) usuários externos
- 2.000 (dois mil) usuários (considerando a estimativa de crescimento)

Justificativa da quantidade:

Em virtude do crescente aumento no acesso à rede devido à expansão do PJE (Processo Judicial Eletrônico), com o aumento significativo de usuários internos e externos, se faz necessário expandir e fortalecer a proteção de firewall para atender essa demanda.

7– ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Objeto: Contratação de empresa para o fornecimento de Solução de Proteção de Rede com características de Next Generation Firewall (NGFW), com assistência e suporte técnico pelo período de 60 (sessenta) meses, bem como os serviços de instalação, treinamento e operação assistida, para atender a demanda do Tribunal Regional Federal da Primeira Região – TRF1.

Link: http://comprasnet.gov.br/livre/Pregao/termohom.asp?prgcod=1118916&co_no_uasg=90027&numprp=52023&codigoModalidade=5&f_lstSrp=T&f_Uf=&f_numPrp=52023&f_coduasg=&f_codMod=5&f_tpPregao=E&f_lstICMS=

Item 1: Adjudicado para: ADISTEC BRASIL INFORMÁTICA LTDA , pelo melhor lance de R$ 1.499.209,32 e a quantidade de 1 Unidade.

Item 2: Adjudicado para: ADISTEC BRASIL INFORMÁTICA LTDA , pelo melhor lance de R$ 996.788,81 e a quantidade de 1 Unidade .

Item 8: Adjudicado para: BLOCKBIT TECNOLOGIA LTDA , pelo melhor lance de R$ 22.000,00 e a quantidade de 1 UNIDADE .

Item	Descrição	Meses	Quantidade	Valor Tota
1	Equipamento Segurança Rede Aplicação: Firewall , Tipo: Ampppliance	60 meses	1	R$ 1.499.209,3
2	Equipamento Segurança Rede Aplicação: Firewall , Tipo: Ampppliance	60 meses	1	R$ 996.788,81
8	SERVIÇO DE TREINAMENTO TÉCNICO OFICIAL (PARA ATÉ OITO ALUNOS), DEMAIS ESPECIFICAÇÕES CONSTAM DO EDITAL E SEUS ANEXOS	-	8 participantes	R$ 22.000,(

Pregão eletrônico 01/2023: Ministério Público do Mato Grosso do Sul

Objeto: Consiste na seleção da proposta mais vantajosa para a Administração, visando a aquisição de solução de segurança de redes de computadores, contendo firewalls de rede, sistema de gerenciamento e emissão de relatórios, sandboxing e autenticação, com serviço de instalação, migração inicial e capacitação, suporte técnico pelo período mínimo de 60 (sessenta) meses, conforme condições, localidades, quantidades e exigências estabelecidas no Termo de Referência e seus adendos (anexo I).

Link: http://comprasnet.gov.br/livre/Pregao/termohom.asp?prgcod=1119370&co_no_uasg=453860&numprp=12023&codigoModalidade=5&f_lstSrp=T&f_Uf=&f_numPrp=12023&f_coduasg=&f_codMod=5&f_tpPregao=E&f_lstICMS

Item 4: Adjudicado para: CLICK TI TECNOLOGIA LTDA , pelo melhor lance de R$ 2.390.000,00.

Item 17: Adjudicado para: CLICK TI TECNOLOGIA LTDA , pelo melhor lance de R$ 120.000,00.

Item	Descrição	Meses	Quantidade	Valor Total
4	Firewall Modelo: Tz670 , Nome: Firewall , Aplicação: Segurança Rede Computadores , Capacidade Armazenamento: Até 32 G	60 meses	1	R$ 2.390.000,0(
17	Treinamento: Firewall de próxima geração	-	-	R$ 120.000,(

PROPOSTAS COMERCIAIS

Empresa COMDADOS

Razão Social: Comdados Comércio e Serviços Eletrônicos Ltda. CNPJ: 34.203.752/0001-71 I.E: 27.099.805NO / I.M.: 36287.5 Endereço: Rua Maria Teixeira de Carvalho,165 – Lot. Bosque dos Kioskes, Qd. A, Lote 27, CEP: 42.701- 880 - Pitangueiras - Lauro de Freitas – Bahia. Site: www.comdados-ba.com.br Telefone Geral: (71) 2202-2838.

Item	Descrição	Meses	Quantidade	Valor Total
1	Solução de Segurança Tipo 2; Modelo FG-2600F + FC-10-F26HF-950-02-60	60 meses	1	R$ 4.742.208,(

Empresa INTELLI WAY

Item	Descrição	Meses	Quantidade	Valor Total
1	Fornecimento de 2 (dois) Firewalls Hillstone modelo A6800 + licenciamento UTM, contemplando garantia pelo fabricante de 36 (trinta e seis) meses Armazenamento: Até 32 G	60 meses	1	R$ 4.326.300,00
2	Fornecimento de 2 (dois) Firewalls Hillstone modelo x8180 + licenciamento UTM, contemplando garantia pelo fabricante de 36 (trinta e seis) meses.	36 meses	1	R$ 5.945.189,40
3	Fornecimento de Serviço de Instalação e Configuração para os firewalls do cenário 1 (A6800) ou cenário 2 (X8180) contemplado nesta proposta.	Pagamento único	-	R$ 123.750,00
4	Suporte Técnico Mensal	36 meses (pagamento por demanda)	-	R$ 356.400,00
5	Fornecimento de Treinamento da solução ofertada nesta proposta para até 5 (cinco) participantes.	-	5 participantes	R$ 16.500,00

CUSTOS TOTAIS

Item	Descrição	TRF 1º	MP/MG	COMDADOS	INTELLI WAY	Valor Total Estimado
		R$ 1.499.209,32	R$ 2.390.000,00	R$ 4.742.208,00	R$ 4.326.300,00 R$ 5.945.189,40	

1	Solução integrada de proteção de rede do tipo “Next Generation Firewall” (NGFW), incluindo fornecimento de licença, transferência de conhecimento, suporte, instalação, implantação e garantia.	R$ 996.788,81 Total R$ 2.495.998,13	Total R$ R$ 2.390.000,00	Total R$ 4.742.208,00	R$ 123.750,00 R$ 356.400,00 Total R$ 10.751.639,40	R$ 5.094.961,38
2	Treinamento informática - sistema , software. De acordo com as especificações do Termo de Referência.	R$ 22.000,00	R$ 120.000,00		R$ R$ 16.500,00	R$ 52.833,33
						Total R$ 5.147.794,71

8– JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

A solução visa implementar um sistema unificado de proteção de borda, que integra diferentes sistemas de proteção de borda, necessitando de tecnologias compatíveis. A aquisição em lote único garante que os equipamentos e tecnologias adquiridas sejam compatíveis entre si, evitando problemas de integração e garantindo a eficiência do sistema de segurança.

Optou-se por manter a solução e o treinamento respectivo em um único lote, pois a separação em lotes distintos da solução e do treinamento da respectiva solução inviabilizaria a licitação do treinamento, pois NÃO é possível licitar o treinamento sem antes saber qual solução adjudicou a licitação.

Portanto, a contratação da solução em lote único é justificada para garantir a compatibilidade das tecnologias, facilitar a integração entre as unidades, bem como proporcionar o treinamento adequado relacionado à solução.

9 – CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Em 2018 foi realizada a Contratação de sistema unificado de proteção de borda, incluindo fornecimento de licença, transferência de conhecimento, suporte, instalação, implantação, garantia e treinamento para o PJES, por meio do processo nº 201500020922.

10- ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO

A presente contratação foi devidamente aprovada pelo Comitê de Governança de Tecnologia da Informação e Comunicação – CGTIC, na forma da ata (1490589) e Processo nº 7001386-44.2023.8.08.0000.

11- RESULTADOS PRETENDIDOS

- Permitir que o Poder Judiciário do Espírito Santo implemente nível adequado de segurança da informação, no que tange às ameaças provenientes de ataques externos e internos;
- Permitir proteção contra ataques maliciosos;
- Diminuir a complexidade na administração da solução;
- Permitir respostas mais rápidas a problemas identificados
- Permitir maior eficiência por meio de atualização tecnológica
- Permitir atendimento das demandas do PJES de curto e médio prazo;
- Aumentar a confidencialidade, integridade e disponibilidade das informações do PJES;
- Capacitar e qualificar a equipe de TI do PJES em tecnologias empregadas;
- Melhorar a imagem do PJES quanto à segurança dos dados.

12- PROVIDÊNCIAS A SEREM ADOTADAS PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

Não há necessidade de adequação do ambiente para viabilizar a contratação de suporte técnico, pois a contratação visa a manter a solução que já se encontra em operação.

13- POSSÍVEIS IMPACTOS AMBIENTAIS E TRATAMENTOS

Os equipamentos e insumos ofertados não deverão conter substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances ou Restrição de Certas Substâncias Perigosas), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs) ou éteres difenil-polibromados (PBDEs).

A CONTRATADA deverá manter programa interno de auto fiscalização da correta manutenção dos equipamentos, bem como adotar política de boas práticas ambientais, especialmente quanto à aquisição e descarte de peças, bem como dos resíduos dos processos de manutenção.

14- DECLARAÇÃO DE VIABILIDADE

A equipe de planejamento declara viável a presente contratação.

Justificativa da Viabilidade:

Conforme demonstrado no item 4, a solução 1, atualmente existente, se mostra impraticável, já defasada, sem funcionalidades, capacidade e desempenho suficientes para operar com um mínimo de segurança..

A solução 2 também é inviável pela necessidade de se utilizar várias soluções para cobrir as funcionalidades necessárias, além da complexidade em si, que exigiria uma equipe dedicada, aumentando consideravelmente os custos da solução.

A solução 4 igualmente se mostra inviável por ser aplicada somente em ambientes de pequeno a médio porte, incompatível com o ambiente atual desde PJES.

Por fim, a solução 3 não apenas aborda as deficiências e limitações da solução existente e das demais apresentadas, mas também eleva significativamente o nível de segurança, disponibilidade e desempenho da rede do Tribunal de Justiça. É uma escolha que visa garantir a proteção dos ativos de informação deste PJES e a continuidade de suas operações de forma eficaz.

Pelo exposto, a equipe de planejamento declara viável a solução 3 para a presente contratação.

Fundamentação para a contratação da solução em lote único

Se tratando de um sistema unificado de proteção de borda integrado é necessário que os tipos de sistemas de proteção de borda possuam tecnologias compatíveis. Além disso, a solução interligará diferentes comarcas e fóruns ao Tribunal de Justiça, desta forma, se faz necessário um lote único para evitar que ocorra a licitação de equipamentos com tecnologias que não sejam compatíveis. Isso comprometeria o projeto de segurança e poderia viabilizar a análise profunda feita pelo IPS, além de dificultar a integração do sistema em si.

Fundamentação para a contratação da solução e do treinamento em lote único

A solução contratada neste termo de referência é considerada comum, por isso a modalidade usada é a de Pregão. Visando a independência do setor público, optou-se por manter a solução e o treinamento respectivo em um único lote, pois a separação em lotes distintos da solução e do treinamento da respectiva solução, inviabilizaria a licitação do treinamento, pois NÃO é possível licitar o treinamento sem antes saber qual solução adjudicou a licitação. A possibilidade de realizar licitações distintas para contratação de treinamento e solução, vai de encontro com o princípio da eficiência e retarda o nivelamento da tecnologia da informação.

Com o intuito de manter a eficiência, eficácia e avançar em direção às metas estabelecidas pelo CNJ, optou-se por manter em um LOTE ÚNICO a solução contratada e o treinamento, visando manter a continuidade do serviço, independente de terceiros e preparar o servidor para a gerência da solução imediatamente após a sua implantação.

15- ANEXOS

Adendo I - Termo de Confidencialidade;
Adendo II - Modelo de proposta comercial;
Adendo III - Especificações Técnicas;
Adendo IV - Termo de Recebimento Definitivo

16- RESPONSÁVEIS

Integrante Demandante: Havirdan das Rodor Araujo

Integrantes Técnicos: Enilson Simões Griffo

Integrante Administrativo: Eduardo Fernandes Leal

Documento assinado eletronicamente por **MARCIANNE RIBEIRO ANTUNES LIMA**, **SECRETARIO DE TECNOLOGIA DA INFORMACAO**, em 07/05/2024, às 13:47, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **EDUARDO FERNANDES LEAL**, **ANALISTA JUD 01 QS AGENTE JUDICIARIO**, em 07/05/2024, às 13:49, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **HAVIRDAN DAS RODOR ARAUJO**, **COORDENADOR DE SUPORTE E MANUTENCAO**, em 07/05/2024, às 15:11, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ENILSON SIMOES GRIFFO**, **TECNICO JUDICIARIO AE TECNICO EM INFORMATICA**, em 16/05/2024, às 14:48, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sistemas.tjes.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2063905** e o código CRC **7160FC10**.