PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR
PRSTM/SECSTM/DITIN/COTEC

ESTUDO TÉCNICO PRELIMINAR

1. ANALISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1.2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.2.1. Identificação das necessidades de negócio

O estudo em questão tem como objetivo avaliar tecnicamente novas tecnologias para atender à crescente demanda de acessos aos sistemas e aplicações que o STM disponibiliza aos seus usuários.

O portal principal do Superior Tribunal Militar (STM) é alvo constante de ataques cibernéticos que visam principalmente indisponibilizar e invadir os sistemas estruturantes

A busca por evolução dos serviços de informática vem resultando em mudanças no perfil de tráfego de suas aplicações internas e externas, exigindo uma revisão da arquitetura de rede atualmente em funcionamento, requerendo dos equipamentos ativos maiores taxas de transmissão e maior poder de processamento.

Tal implementação requer uma maior interatividade da parte de gerência entre os sistemas, procedimentos de configuração, desempenho, qualidade e recuperação da informação, bem como a total interoperabilidade, visando uniformização dos recursos como um todo.

Nesse sentido, a adoção de tecnologias modernas e inovadoras, como Web Application Firewall de alto desempenho e segurança da informação aplicada às camadas superiores, é fundamental para garantir a segurança do datacenter do STM.

Busca-se contratar uma solução de proteção de aplicações e balanceamento de carga (WAF) O serviço de balanceamento de carga de aplicativos atende à alta disponibilidade de rede e ao aumento do desempenho, permitindo maior governança, confiabilidade e escalabilidade aos serviços de TI fornecidos pelo STM.

Além disso, com a aquisição de uma solução de proteção de aplicações e balanceamento de carga (WAF), será possível disponibilizar uma estrutura mais robusta e confiável para que os servidores possam desempenhar suas funções adequadamente.

1.2.2. Identificação das necessidades tecnológicas

a) A solução de proteção de aplicações e balanceamento de carga (WAF) deve ser capaz de lidar com possíveis contingências e falhas, distribuindo de forma eficiente todas as conexões recebidas pelos sistemas provenientes do datacenter do STM. Isso assegurará a confiabilidade e disponibilidade das informações.

b) É essencial que a solução proporcione um Gerenciamento de Tráfego que permita o acesso rápido e seguro, otimizando o desempenho dos aplicativos. Além disso, deve estabelecer limites para Transações Por Segundo (TPS), velocidade de encriptação SSL e suportar uma alta quantidade de conexões concorrentes.

c) É desejável que a solução simplifique o gerenciamento por meio de uma interface intuitiva, fornecendo uma visibilidade granular de todo o tráfego. Isso permitirá suporte rápido a mudanças e customizações em diferentes implementações.

d) A solução deve ser capaz de controlar o fluxo das aplicações, permitindo uma inspeção completa do tráfego e um gerenciamento programável para atender e agir de acordo com o fluxo das aplicações.

e) É importante que a solução possibilite a garantia de prioridade para aplicações prioritárias, por meio do controle das aplicações, acelerando o acesso e melhorando seu desempenho.

f) A solução deve aprimorar a proteção e segurança de rede e aplicativos, adicionando funções críticas de segurança que não podem ser delegadas a nenhum componente do ambiente de rede.

g) Além disso, é desejável que a solução otimize a banda de acesso, aliviando a carga sobre os servidores de rede.

h) A solução deve ser compatível com as novas tecnologias já existentes no STM, permitindo sua substituição ou atualização sem impactos negativos.

j) É fundamental que a solução forneça o balanceamento de carga entre os servidores, garantindo uma distribuição equilibrada do tráfego.

k) A solução deve oferecer monitoramento do uso do usuário final, permitindo uma análise detalhada do comportamento e das demandas dos usuários.

l) Além disso, a solução deve gerenciar eventuais lentidões nas aplicações e no banco de dados, identificando e solucionando possíveis gargalos.

m) É importante que a solução verifique a existência de gargalos nas transações das aplicações, na infraestrutura ou na integração, possibilitando a identificação e correção desses problemas.

n) O gerenciamento dos registros dos dados do aplicativo também deve ser contemplado pela solução, garantindo uma gestão eficiente e segura dessas informações.

o) A solução deve ser capaz de evitar e corrigir erros nas aplicações, sem a necessidade de o usuário reportar qualquer tipo de problema.

p) A solução deve ser capaz também de interagir com servidores de autenticação, autorização e auditoria (AAA) que contêm informações do usuário.

q) proteger contra os 10 principais da OWASP, e todas as outras ameaças aos sistemas e aplicações como: ataques DDoS, ataques ativados por bot, roubo de propriedade intelectual e fraude.

r) Por fim, a solução deve gerar eficiência, proporcionando um ambiente de TI mais ágil, seguro e escalável para o STM, otimizando recursos e maximizando a produtividade da equipe de TI.

1.2.3. Demais requisitos necessários e suficientes à escolha da solução de TIC

Uma das necessidades urgentes do Superior Tribunal Militar é na adoção de mecanismos de segurança da informação e a utilização de recursos de inspeção e proteção do tráfego de dados que auxiliem, de forma proativa, a prevenção das vulnerabilidades encontradas em diversos vetores – redes (perímetro), sistemas de mensagens eletrônicas (e-mail), sistemas e aplicativos, servidores de aplicação, e infraestruturas.

A atenção relativa à segurança deve ser dispensada não somente aos sistemas informatizados, mas também às informações que esses sistemas recebem, processam, divulgam e descartam. Na sociedade da informação vivida nos tempos atuais, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão estas sob constantes riscos e necessitam ser adequadamente protegidas. Com isso, a Segurança da Informação tornou-se um ponto crucial para a sobrevivência e credibilidade das instituições.

No ano de 2022 o Superior Tribunal Militar sofreu um total de 167.500 tentativas de ataques ao seu portal externo.

O Superior Tribunal Militar trata diariamente um grande volume de dados sensíveis e processos de trabalho, para os quais precisa garantir confidencialidade, disponibilidade e integridade destas informações. De outro lado, a partir da ampliação da transformação digital e a disponibilização das soluções de software baseadas nos protocolos que constituem a Web, principalmente, HTTP (HyperText Transfer Protocol) e HTTPS (HyperText Transfer Protocol Secure) para acessos externos e internos, respectivamente, via Internet e Intranet, tornou-se necessário reduzir a superfície de ataque, ampliando a segurança da informação deste egrégio Superior Tribunal Militar, uma vez que tais aplicações são vetores potenciais para exploração de falhas, principalmente ao se considerar a complexidade das arquiteturas de softwares e plataformas utilizadas.

Neste cenário, a maioria das ameaças explora vulnerabilidades existentes em aplicações, dentre outras. Por isso, é necessária a contratação de uma solução que possa, de forma customizada ao ambiente, interceptar e mitigar o risco inerente aos sistemas. O alvo dos atacantes geralmente são vulnerabilidades em sistemas desatualizados, legados ou com falhas no desenvolvimento. Por meio dessas brechas, são realizados diversos tipos de ataques, visando espionagem, vazamento de dados, roubo de informações ou quebra de integridade e disponibilidade do ambiente.

Além do risco de vazamento de dados sensíveis, existe a preocupação de que a sociedade perca a confiança nos serviços disponibilizados, entre outras inúmeras consequências à imagem do Superior Tribunal Militar. Para que seja alcançado o nível de segurança exigido atualmente, é necessário investir em processos, sistemas e conhecimento específicos contra ameaças avançadas.

Diante disso, o Superior Tribunal Militar identificou a necessidade de contratação e implantação de solução de segurança que permita realizar a proteção das aplicações da Internet/Intranet, bem como a adoção de medidas rigorosas de segurança para controle do acesso aos sistemas críticos. Portanto, para identificar e evitar ataques destinados a explorar recursos de camada de aplicação, considerando o modelo de referência Open System Interconnection definido pela International Organization for Standardization (ISO/OSI), são necessárias ferramentas especializadas como as soluções Web Application Firewall - WAF com suporte de segurança a APIs (Application Program Interfaces). A solução WAF, ou Firewall de Aplicação Web, é uma solução que fica entre o site ou aplicativo e o restante da internet e a rede interna, funcionando como uma barreira que bloqueia e protege o ambiente de aplicações contra-ataques de Hackers, Spammers, DDoS, Injeções SQL, proteção contra captura de dados sensíveis e roubo de credenciais, proteção contra raspagem de dados realizadas através de robôs (bots) maliciosos e muito outros tipos de Cyber Ataques.

A implementação dessa solução tem também como objetivo, aprimorar substancialmente o nível de segurança da informação do STM, elevando os padrões de proteção e garantindo a integridade, confidencialidade e disponibilidade dos dados sensíveis. Ao fornecer visibilidade das aplicações e dos riscos associados a elas, essa solução permite que a equipe de segurança da informação tenha um panorama completo do ambiente. Isso possibilita uma análise mais precisa e eficiente das ameaças e vulnerabilidades, permitindo a implementação de medidas proativas para mitigar potenciais ataques e incidentes de segurança.

Dessa forma, visando alinhamento estratégico e ganho em escalabilidade, disponibilidade, confiabilidade na entrega dos serviços prestados aos usuários, o Superior Tribunal Militar pretende adquirir uma solução de Web Application Firewall (WAF) que compreende a função de proteção avançada de aplicações, atue como proxy, DNS e balanceamento de tráfego o que proporciona uma gestão abrangente e uma visibilidade aprimorada das vulnerabilidades e dos dispositivos presentes no ambiente do STM. Isso permite a identificação e o tratamento eficiente de eventuais pontos fracos, reduzindo as possibilidades de exploração por parte de atacantes.

Além dos aspectos de segurança, essa solução visa melhorar a experiência do usuário no acesso externo ao ambiente do STM. Ao proporcionar uma conexão mais segura, estável e rápida, os usuários externos terão uma navegação mais fluida e eficiente, facilitando o seu trabalho e aumentando a produtividade. A solução também inclui recursos avançados de gerenciamento de aplicações, com a implementação de políticas e controles baseados nas normativas de segurança e na Lei Geral de Proteção de Dados (LGPD). Isso garante que as aplicações sejam configuradas de acordo com as melhores práticas de segurança e que o tratamento dos dados pessoais esteja em conformidade com a legislação vigente.

1.2.4. Requisitos sociais, ambientais e culturais

1.2.4.1. A prestação dos serviços pela empresa CONTRATADA deve sempre ser pautada pelo uso racional de recursos e equipamentos, visando evitar e prevenir o desperdício de insumos e materiais. É necessário adotar práticas que promovam a eficiência e a sustentabilidade, contribuindo para a otimização dos recursos disponíveis.

1.3. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS E JUSTIFICATIVA DA CONTRATAÇÃO

1.3.1. Estima-se a aquisição de equipamentos do tipo Web Application Firewall para formação de um cluster para operação no STM. Os quantitativos pretendidos estão dispostos na tabela abaixo, sendo que o cluster deverá ser composto por dois appliances físicos, conforme solução disponível. Inclui-se, ainda, garantia de 60 meses, serviços de implantação, instalação e configuração do cluster e treinamento para capacitação técnica da equipe interna do Superior Tribunal Militar.

	ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTDE.
GRUPO 1	1	Solução de Proteção de Aplicações e Balanceamento de Carga (WAF) com Suporte Especializado e garantia pelo período de 60 (sessenta) meses.	UN	2
	2	Serviço de Implantação e configuração da solução.	UN	1
	3	Treinamento	UN	6

1.4. ANÁLISE DE SOLUÇÕES

1.4.1. Disponibilidade de solução similar em outro órgão ou entidade da Administração Público

1.4.1.1. A solução analisada é bem comum, encontrada em diversos órgãos e entidades públicos. A pesquisa de preços, anexo deste processo administrativo, indica diversos órgãos com contratações similares. Vários órgãos na Administração Pública Federal possuem essa solução em operação. O que pode diferir é a capacidade de processamento de cada equipamento que corresponderá ao dimensionamento de cada órgão.

1.4.2. Identificação das possíveis soluções.

ID	DESCRIÇÃO DA SOLUÇÃO
1	Contratação de solução baseada em software livre.
2	Modelo de computação em nuvem baseado em IaaS (Infraestrutura como Serviço) que é disponibilizado através de um software hospedado na infraestrutura do provedor, permitindo que seja contratado de acordo com a demanda ou mediante o uso mensal do serviço.
3	Aquisição de uma solução de proteção de aplicações (WAF) com balanceamento de carga e outras funcionalidades.

1.4.3. Análise comparativa das soluções.

ID	SOLUÇÃO	ORGÃO/PREGÃO	SERVIÇOS EXECUTADOS	QNTD	VALOR TOTAL R$
1	OBJETO DA PRESENTE LICITAÇÃO É O REGISTRO DE PREÇOS PARA ESCOLHA DA PROPOSTA MAIS VANTAJOSA PARA A CONTRATAÇÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO PARA AQUISIÇÃO DE SOLUÇÃO DE APPLICATION DELIVERY CONTROLLER (ADC), CONFORME CONDIÇÕES, QUANTIDADES E EXIGÊNCIAS ESTABELECIDAS NESTE EDITAL E SEUS ANEXOS.	INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA 08/2021	Application Delivery Controller (ADC)	8	R$16,465.720,00
			Plataforma de Gerenciamento para ADC	3	
			Instalação e Configuração para ADC	4	
			Semana de Operação Assistida para ADC	14	
			Transferência de Conhecimento para ADC	6	
			Banco de Horas de Consultoria Especializada	1240	
			Garantia e Suporte Técnico para ADC (60 meses)	8	
			Garantia e Suporte Técnico para Plataforma deGerenciamento para ADC (60 meses)	3	
2	FORNECIMENTO E IMPLANTAÇÃO DE SOLUÇÃO DE BALANCEAMENTO DE CARGA (APPLICATION DELIVERY CONTROLLER - ADC) PARA APLICAÇÕES, SITES E SERVIÇO DE	COMPANHIA DE SANEAMENTO BÁSICO DO ESTADO DE SÃO PAULO - 656/2021	BALANCEADORES DE CARGA	1	R$4.030.000,00
			LICENÇA DE SOFTWARE		
			INSTALAÇÃO E CONFIGURAÇÃO		
			SUPORTE TÉCNICO		
			APOIO TÉCNICO SOB DEMANDA		
			TREINAMENTO		
4	O OBJETO DA PRESENTE LICITAÇÃO É A ESCOLHA DA PROPOSTA MAIS VANTAJOSA PARA A CONTRATAÇÃO DE SOLUÇÃO DE EQUIPAMENTOS	MINISTÉRIO DO DESENVOLVIMENTO REGIONAL – MDR 11/2022	Solução de balanceamento de carga, Web Application Firewall e DNS do TIPO I (Bloco E), com garantia e suporte técnico para 60 meses.	2	R$4.437.000,00

	FIREWALL DE PRÓXIMA GERAÇÃO E FIREWALL DE APLICAÇÃO WEB, BALANCEADOR DE CARGA E PUBLICADOR DE DNS, PARA PROTEÇÃO DO PERÍMETRO DA REDE DE DADOS, DOS ATIVOS DE HARDWARE E SOFTWARE E DAS APLICAÇÕES WEB DO MINISTÉRIO, COMPREENDENDO GERÊNCIA CENTRALIZADA, INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO, COM GARANTIA E SUPORTE TÉCNICO PELO PERÍODO DE 60 (SESSENTA)MESES, CONFORME CONDIÇÕES, QUANTIDADES E EXIGÊNCIAS ESTABELECIDAS NESTE EDITAL E SEUS ANEXOS.		Solução de balanceamento de carga, Web Application Firewall e DNS do TIPO II (CENAD) com garantia e suporte técnico para 60 meses.	2	
			Gerência Centralizada da solução de Web Appllication Firewall (WAF), balanceamento de carga e DNS com garantia e suporte por 60 meses.	1	
			Serviço de Instalação e Configuração da solução de firewall de aplicação web e gerência centralizada	1	
5	REGISTRO DE PREÇOS DE SOLUÇÃO DE WEB APPLICATION FIREWALL (WAF) EBALANCEAMENTO DE CARGA, INCLUINDO PRESTAÇÃO DE SERVIÇOS DEINSTALAÇÃO E CONFIGURAÇÃO, TREINAMENTO ESPECIALIZADO E SERVIÇO DEOPERAÇÃO ASSISTIDA, COM GARANTIA TÉCNICA DE 60 (SESSENTA) MESES	TRIBUNAL REGIONAL ELEITORAL TRE-PA 46/2022	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL, COM GARANTIA DE 60(SESSENTA) MESES.	28	R$36.928.839,00
			FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO, COM GARANTIA DE 60(SESSENTA) MESES.	20	
			CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB	28	
			SERVIÇO DEINSTALAÇÃO EREPASSE DECONHECIMENTOHANDS-ON	20	
			TREINAMENTOESPECIALIZADO	90	
			SERVIÇO DE OPERAÇÃOASSISTIDA	19	
6	AQUISIÇÃO DE CLUSTER DE APPLICATION DELIVERY CONTROLLER (ADC), SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO, COM FUNÇÕES DE BALANCEADOR DE CARGA E ACELERAÇÃO WEB COM MÓDULOS DE LOADING BALANCE, GLOBAL SERVER LOADING BALANCE, WEB APPLICATION FIREWALL E SSL OFFLOAD E INSPECTION (LB/GSLB/WAF/SSL), INCLUINDO GARANTIA E SUPORTE TÉCNICO ESPECIALIZADO DE 60 (SESSENTA) MESES E SERVIÇOS AGREGADOS DE INSTALAÇÃO/MIGRAÇÃO E TREINAMENTO, PARA ATENDER ÀS NECESSIDADES DO MINISTÉRIO DAS RELAÇÕES EXTERIORES (MRE), CONFORME	MINISTÉRIO DAS RELAÇÕES EXTERIORES – MRE 08/2022	Cluster de Application Delivery Controller (ADC), com funções de balanceador de carga e aceleração web com módulos de Loading Balance, Global Server Loading Balance, Web Application Firewall e SSL offload e inspection (LB/GSLB/WAF/SSL), incluindo garantia e suporte técnico especializado de 60 (sessenta) meses	1	R$3.690.000,00
			Serviços de implantação, instalação e configuração da solução Cluster ADC	1	
			Provimento de 30 horas treinamento para capacitação técnica da equipe interna e transferência de conhecimento acerca da solução a	1	

	CONDIÇÕES, QUANTIDADES E EXIGÊNCIAS ESTABELECIDAS NESTE EDITAL E EM SEUS ANEXOS.		ser adquirida no escopo desta contratação.		

1.4.3.1. A existência de software público brasileiro

1.4.3.1.1. De acordo com a busca realizada com as palavras chaves de Balanceamento e Load Balance, o portal: softwarepublico.gov.br, retornou que não havia encontrado nenhum software correspondente.

1.4.3.1.2. As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg CP-Brasil e e-ARQ Brasil, quando aplicáveis;

Requisito	**Solução**	**Sim**	**Não**	**Não se Aplica**
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3		X	
A Solução está disponível no Portal do Software Público Brasileiro?(quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
A Solução é aderente às regulamentações da ICP-Brasil?(quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

1.5. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

1.5.1. Solução de ID 01 Compreende o uso de solução baseada em software livre. Devido à falta de suporte técnico especializado, possuir código fonte, ausência de garantias e necessidade de composição com vários produtos para entrega aproximada da necessidade, fica evidente que não atenderia ao processo de contratação.

1.5.2. Solução de Id 02 Compreende a adoção de um modelo de infraestrutura em nuvem e exigirá uma análise detalhada das opções disponíveis, bem como a gestão adequada dos riscos relacionados ao tratamento de dados, em conformidade com as diretrizes estabelecidas pela LGPD. Essa transição poderia implicar em grandes mudanças na topologia do STM e na necessidade de migrar toda a infraestrutura para esse modelo. No entanto, no momento atual, não há planos para uma transição completa para a infraestrutura em nuvem devido a considerações relacionadas ao modelo de negócio. Além disso, a administração pública como um todo ainda não possui maturidade suficiente para absorver plenamente esse tipo de serviço, além de não contar com mão de obra especializada para suportá-lo, o que torna sua utilização inviável no momento. No entanto, o fator decisivo para a exclusão dessa possibilidade foi a natureza crítica dos dados que trafegam na rede do Superior Tribunal Militar, tal modalidade iria exigir uma abordagem de segurança mais cautelosa, além de não oferecer proteção contra ataques originados diretamente na rede do STM onde o tráfego da rede interna não seria inspecionado dentro da rede local o que acaba dificultando a implementação dessa boa prática de segurança, já que o tráfego precisaria sair da rede interna para ser inspecionado gerando maior atraso e expondo esse tráfego o que significa maior risco á integridade e vazamento de informações.

1.6. ANÁLISE COMPARATIVA DE CUSTOS (Total Cost Ownership – TCO

1.6.1. Análise Comparativa de Custos (Total Cost Ownership – TCO

1.6.1.1. Ao elaborar o Custo Total de Propriedade (TCO) de cada um dos itens, foi levado em conta os seguintes itens:

	ITEM	**DESCRIÇÃO**	**UNIDADE DE MEDIDA**	**QTDE.**
GRUPO 1	1	Solução de Proteção de Aplicações e Balanceamento de Carga (WAF) com Suporte Especializado e garantia pelo período de 60 (sessenta) meses.	UN	2
	2	Serviço de Implantação e configuração da solução.	UN	1
	3	Treinamento	UN	6

1.6.1.2. **TCO ITEM 1.** Para realização deste TCO, realizou-se pesquisa de preço de aquisições e contratações similares de outros entes públicos, quais sejam:

PREGÃO	SOLUÇÃO	VALOR TOTAL R$	VALOR MÉDIA TOTAL R$
INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA 08/2021	2 (dois) Appliances compondo 1 (um)Cluster	R$2.170.000,00	R$3.403.539,20
COMPANHIA DE SANEAMENTO BÁSICO DO ESTADO DE SÃO PAULO - 656/2021		R$3.534.900,00	
MINISTÉRIO DAS RELAÇÕES EXTERIORES – MRE 08/2022		R$7.060.000,00	
MINISTÉRIO DO DESENVOLVIMENTO REGIONAL – MDR 11/2022		R$2.580.000,00	
TRIBUNAL REGIONAL ELEITORAL TRE-PA 46/2022		R$1.672.796,00	

1.6.1.3. **TCO ITEM 2.** Para realização deste TCO, realizou-se pesquisa de preço de aquisições e contratações similares de outros entes públicos, quais sejam:

PREGÃO	IMPLENTAÇÃO	VALOR TOTAL R$	VALOR MÉDIA TOTAL R$
INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA 08/2021	Serviço de Implantação e configuração da solução 2 (dois) Appliances compondo 1 (um)Cluster	R$189.000,00	R$177.666,67
MINISTÉRIO DO DESENVOLVIMENTO REGIONAL – MDR 11/2022		R$80.000,00	
MINISTÉRIO DAS RELAÇÕES EXTERIORES – MRE 08/2022		R$84.000,00	

1.6.1.4. **TCO ITEM 3.** Para realização deste TCO, realizou-se pesquisa de preço de aquisições e contratações similares de outros entes públicos, quais sejam:

PREGÃO	TREINAMENTO	VALOR TOTAL R$	VALOR MÉDIA TOTAL R$
INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA 08/2021	TREINAMENTO (TURMA 6 PESSOAS)	R$165.600,00	R$119.783,33
TRIBUNAL REGIONAL ELEITORAL TRE-PA 46/2022		R$117.750,00	
MINISTÉRIO DAS RELAÇÕES EXTERIORES – MRE 08/2022		R$76.000,00	

1.6.1.5. **TCO Propostas.** Para realização deste TCO, realizou-se pesquisa de preço com as empresas que ofertam a solução, quais sejam:

a) Empresa NVIA

	ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTDE.	VALOR UNITÁRIO	VALOR TOTAL
GRUPO 1	1	Solução de Proteção de Aplicações e Balanceamento de Carga (WAF) com Suporte Especializado e garantia pelo período de 60 (sessenta) meses.	UN	2	R$ 1.700.000,00	R$ 2.400.000,0
	2	Serviço de Implantação e configuração da solução.	UN	1	R$ 60.000,00	R$ 60.000,00
	3	Treinamento	UN	6	R$ 25.000,00	R$ 150.000,00
	4	Suporte Especializado pelo período de 60 (sessenta) meses.	Mensal	60	R$ 10.000,00	R$ 600.000,00
	TOTAL					R$ 3.210.000,00

b) Global Sec

	ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTDE.	VALOR UNITÁRIO	VALOR TOTAL
GRUPO 1	1	Solução de Proteção de Aplicações e Balanceamento de Carga (WAF) com Suporte Especializado e garantia pelo período de 60 (sessenta) meses.	UN	2	R$ 1.450.000,00	R$ 2.900.000,00
	2	Serviço de Implantação e configuração da solução.	UN	1	R$ 85.000,00	R$ 85.000,00
	3	Treinamento	UN	6	R$ 28.000,00	R$ 168.000,00
	4	Suporte Especializado pelo período de 60 (sessenta) meses.	Mensal	60	R$ 8.200,00	R$ 492.000,00
	TOTAL					R$ 3.645.000,00

c) VTECH

	ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTDE.	VALOR UNITÁRIO	VALOR TOTAL
GRUPO 1	1	Solução de Proteção de Aplicações e Balanceamento de Carga (WAF) com Suporte Especializado e garantia pelo período de 60 (sessenta) meses.	UN	2	R$ 1.390.000,00	R$ 2.780.000,00
	2	Serviço de Implantação e configuração da solução.	UN	1	R$ 66.100,00	R$ 66.100,00
	3	Treinamento	UN	6	R$ 20.000,00	R$ 120.000,00
	4	Suporte Especializado pelo período de 60 (sessenta) meses.	Mensal	60	R$ 15.000,00	R$ 900.000,00
	TOTAL					R$ 3.866.100,00

d) LAYER

	ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTDE.	VALOR UNITÁRIO	VALOR TOTAL
GRUPO 1	1	Solução de Proteção de Aplicações e Balanceamento de Carga (WAF) com Suporte Especializado e garantia pelo período de 60 (sessenta) meses.	UN	2	R$ 1.400.000,00	R$ 2.800.000,00
	2	Serviço de Implantação e configuração da solução.	UN	1	R$ 80.000,00	R$ 80.000,00
	3	Treinamento	UN	6	R$ 30.000,00	R$ 180.000,00
	4	Suporte Especializado pelo período de 60 (sessenta) meses.	Mensal	60	R$ 13.500,00	R$ 810.000,00
	TOTAL					R$ 3.870.000,00

1.7. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Aquisição de solução de proteção de aplicações e balanceamento de carga (WAF), incluindo prestação de serviços de instalação e configuração, com garantia técnica de 60 (sessenta) meses, bem como treinamento para capacitação técnica de servidores do Superior Tribunal Militar. Incluindo suporte técnico especializado de 60 (sessenta) meses e serviços agregados de migração, para atender às necessidades do STM conforme condições e especificações estabelecidas no Termo de Referência e em seus anexos.

A Solução selecionada, identificada como ID 03, inclui a aquisição de uma solução de firewall de aplicação Web (WAF), juntamente com o balanceador de carga, e terá como objetivo principal fornecer proteção abrangente contra ataques de camada de aplicação, ataques DNS e ataques de negação de serviço. Além disso, essa solução permitirá a publicação otimizada das aplicações do STM na Internet, garantindo uma experiência eficiente para os usuários, ao mesmo tempo em que equilibra o tráfego das aplicações entre os ativos de infraestrutura e rede do STM.

	ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTDE.
GRUPO 1	1	Solução de Proteção de Aplicações e Balanceamento de Carga (WAF) com Suporte Especializado e garantia pelo período de 60 (sessenta) meses.	UN	2
	2	Serviço de Implantação e configuração da solução.	UN	1
	3	Treinamento	UN	6
	4	Suporte Especializado pelo período de 60 (sessenta) meses.	Mensal	60

1.7.1. Requisitos técnicos - item 1

1.7.1.1. Especificação técnica mínima

1.7.1.1.1. Os appliances físicos devem ser novos e de primeiro uso;

1.7.1.1.2. Os equipamentos devem ser fornecidos em modo appliance, com conjunto de hardware e software dedicados, não podendo ser servidor de uso genérico, e que atendam todas as funcionalidades descritas neste Termo de Referência.

1.7.1.1.3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie.

1.7.1.1.4. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante.

1.7.1.1.5. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2Us do referido rack;

1.7.1.1.6. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos"), incluindo todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento do equipamento no rack;

1.7.1.1.7. Deve ser fornecido com todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento.

1.7.1.1.8. Dispor de fonte de alimentação redundante com tensão de entrada de 110V a 220V AC automática e frequência de 60Hz;

1.7.1.1.9. Possuir sistema operacional customizado especificamente para funções de Web Application Firewall, não podendo ser entregue appliance do tipo NGFW;

1.7.1.1.10. Possuir, no mínimo, 06 interfaces, sendo 04 de 10GE RJ45 e 2 interfaces 10GE Fibra SFP+ SR; serão aceitas interfaces de maior capacidade, desde que possibilitem ser transformados em 10 GE (incluindo os cabos “breakout” de no mínimo 3 metros;

1.7.1.1.11. Possuir 01 interfaces 1GE, incluso interfaces de gerência com conectores padrão RJ45;

1.7.1.1.12. Todas as interfaces fornecidas devem estar licenciadas e habilitadas para uso imediato;

1.7.1.1.13. Possuir no mínimo de 17 Gbps de throughput em camada 7;

1.7.1.1.14. Possuir capacidade de operar, no mínimo, 800 mil conexões por segundo na camada 7;

1.7.1.1.15. Possuir capacidade de operar, no mínimo, 300 mil conexões por segundo na camada 4;

1.7.1.1.16. Possuir capacidade de 10.000 transações por segundo (TPS) em TLS padrão RSA (chaves de 2.048 bit);

1.7.1.1.17. Possuir no mínimo 15 Gbps de compressão em hardware;

1.7.1.1.18. Recursos de agregação de portas baseado no protocolo LACP, segundo o padrão IEEE 802.3ad;

1.7.1.1.19. Memória RAM mínima de 32 GB;

1.7.1.1.20. Disco rígido com capacidade de armazenamento interno e retenção de logs para análise ser de no mínimo 480 GB;

1.7.1.1.21. Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados seja realizada com aceleração em hardware, para não onerar o sistema

1.7.1.1.22. Suportar e garantir a instalação em ambiente de alta disponibilidade;

1.7.1.1.23. Deve permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo e ativo-ativo.

1.7.1.1.24. A solução deve suportar mais do que dois elementos no cluster para sincronização de configuração de forma nativa a fim de permitir escalabilidade no futuro.

1.7.1.1.25. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades.

1.7.1.1.26. Deve possuir redundância de dispositivos, de maneira que, em caso de falha de um dos equipamentos, o estado de todas as conexões seja remanejado para o equipamento redundante, preservando o estado original de todas as tabelas de conexões e de persistência.

1.7.1.1.27. O equipamento deve permitir a sincronização das configurações de forma automática.

1.7.1.1.28. Caso seja necessária uma interligação entre os equipamentos, a CONTRATADA será integralmente responsável por tal interligação, garantindo a performance necessária para o atendimento da solução.

1.7.1.1.29. O equipamento, quando habilitado para mais de uma função (Balanceamento, DNS, Web Application Firewall, etc), deverá permitir a definição da importância da função para cada tipo de funcionalidade;

1.7.1.1.30. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, WAF, etc.

1.7.1.1.31. Fornecer recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

1.7.1.1.32. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e HTTP/3;

1.7.1.1.33. Possuir suporte a IPv6;

1.7.1.1.34. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

1.7.1.1.35. Deve suportar, no mínimo, 1000 VLANs simultaneamente;

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

1.7.1.1.37. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).

1.7.1.1.38. Assinar cookies digitalmente e editar endereços de URL (“URL Rewriting”);

1.7.1.1.39. O equipamento deverá permitir a sincronização das configurações:

1.7.1.1.39.1. De forma automática;

1.7.1.1.39.1.2. Manualmente, forçando a sincronização apenas no momento desejado;

1.7.1.1.40. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

1.7.1.1.40.1.1. Compartilhar a rede de heartbeat com a rede de dados;

1.7.1.1.40.1.2. Utilizar uma rede exclusiva para o heartbeat.

1.7.1.1.41. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;

1.7.1.1.42. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

1.7.1.1.43. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

1.7.1.1.44. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

1.7.1.1.45. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version

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

1.7.1.1.47. Deve implementar configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para a interface de gerenciamento

1.7.1.1.48. Permitir acesso in-band via SSH

1.7.1.1.49. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.

1.7.1.1.50. Possuir console de administração com interface gráfica remota segura atendendo os seguintes requisitos:

1.7.1.1.50.1.1. Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e logs;

1.7.1.1.50.1.2. Permitir a replicação de configurações e a aplicação de atualização de softwares para os elementos dos nós do cluster;

1.7.1.1.51. Manter internamente múltiplos arquivos de configurações do sistema;

1.7.1.1.52. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;

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

1.7.1.1.54. Deverá ser possível associar aos usuários de bases externas como RADIUS, LDAP e TACACS+ o nível de acesso;

1.7.1.1.55. Possuir Interface Gráfica via Web;

1.7.1.1.56. Possuir auto-complementação de comandos na CLI;

1.7.1.1.57. Possuir ajuda contextual;

1.7.1.1.58. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;

1.7.1.1.59. A Solução deve ter suporte a sFlow;

1.7.1.1.60. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;

1.7.1.1.61. Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;

1.7.1.1.62. A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;

1.7.1.1.63. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;

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

1.7.1.1.65. Suportar a rollback de configuração e imagem;

1.7.1.1.66. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;

1.7.1.1.67. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

1.7.1.1.68. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;

1.7.1.1.69. A interface Gráfica deverá permitir a reinicialização do equipamento;

1.7.1.1.70. Reinicialização do equipamento por comando na CLI;

1.7.1.1.71. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;

1.7.1.1.72. Possuir traps SNMP;

1.7.1.1.73. Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events;

1.7.1.1.74. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;

1.7.1.1.75. Implementar Debugging: CLI via console e SSH;

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

1.7.1.1.77. Permitir a criação de políticas diferenciadas por aplicação.

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

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

1.7.1.1.80. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

1.7.1.1.81. Permitir as seguintes opções de implementação:

1.7.1.1.82. Monitoramento (sem bloqueio);

1.7.1.1.83. Proxy (reverso e transparente).

1.7.1.1.84. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;

1.7.1.1.85. Remover as mensagens de erro do conteúdo que será enviado aos usuários;

1.7.1.1.86. Em modo “monitoramento” (sem bloqueio), realizar análise e avaliação do tráfego, gerar relatórios com os dados analisados e simular bloqueios para efeito de avaliação;

1.7.1.1.87. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos;

1.7.1.1.88. Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:

1.7.1.1.88.1. Identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações;

1.7.1.1.89. Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;

1.7.1.1.90. A solução deve suportar e fazer a proteção do tráfego de protocolo WebSocket.

1.7.1.1.91. A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automatica

1.7.1.1.92. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além de proteção contra- ataques conhecidos aos protocolos HTTP e HTTPS;

1.7.1.1.93. Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão;

1.7.1.1.94. Bloqueio com intermediação e interrupção da conexão;

1.7.1.1.95. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;

1.7.1.1.96. Utilização de página HTML informativa e personalizável como HTTP Response aos bloqueios;

1.7.1.1.97. Configuração de políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação;

1.7.1.1.98. Permitir apenas transações de aplicações validadas, o restante das transações deverá ser bloqueado, utilizando bloqueio por nível de aplicação baseado no contexto da sessão do usuário, com privilégios de autorização diferentes, entradas de usuários e tempo de resposta de aplicação;

1.7.1.1.99. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:

1.7.1.1.99.1. Endereços IP que originaram os ataques;

1.7.1.1.99.2. Horário do ataque;

1.7.1.1.99.3. Nome do ataque;

1.7.1.1.99.4. Qual campo foi atacado;

1.7.1.1.99.5. Quantas vezes esse ataque foi realizado;

1.7.1.1.100. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório), cookies, ações SOAP e elementos XML; identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP;

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

1.7.1.1.102. Identificar ataques baseados em:

1.7.1.1.102.1. Assinaturas, com atualização diária da base pelo fabricante;

1.7.1.1.102.2. Regras;

1.7.1.1.102.3. Perfis de utilização;

1.7.1.1.103. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em analise comportamental, usando o aprendizado.

1.7.1.1.104. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser auto-ajustáveis e adpatativos de acordo com mudanças.

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

1.7.1.1.106. Detectar ataques de força bruta por meio dos seguintes métodos:

1.7.1.1.107. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;

1.7.1.1.108. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP.

1.7.1.1.109. Detectar ataques do tipo força bruta em que:

1.7.1.1.109.1. O atacante solicita repetidamente o mesmo recurso;

1.7.1.1.109.2. O atacante realiza repetidas tentativas não autorizadas de acesso;

1.7.1.1.109.3. São utilizados ataques automatizados de login.

1.7.1.1.110. Detectar ataques do tipo força bruta que explorem:

1.7.1.1.110.1. Controles de acesso da aplicação (Erro 401 – Unauthorized);

1.7.1.1.110.2. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação;

1.7.1.1.110.3. Aplicações WEB que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação);

1.7.1.1.110.4. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de Ips);

1.7.1.1.110.5. Clientes automatizados (robôs, requisições muito rápidas);

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

1.7.1.1.110.7. Possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bidirecional atravessando o equipamento;

1.7.1.1.110.8. Possibilitar atualização de novas assinaturas para ataques conhecidos;

1.7.1.1.111. Apresentar proteção contra-ataques, como:

1.7.1.1.111.1. Brute Force Login;

1.7.1.1.111.2. Buffer Overflow;

1.7.1.1.111.3. Cookie Injection;

1.7.1.1.111.4. Cookie Poisoning;

1.7.1.1.111.5. Cross Site Request Forgery (CSRF);

1.7.1.1.111.6. Cross Site Scripting (XSS);

1.7.1.1.111.7. Server Side Request Forgery (SSRF)

1.7.1.1.111.8. Directory Traversal;

1.7.1.1.111.9. Forceful Browsing;

1.7.1.1.111.10.HTTP Denial of Service;

1.7.1.1.111.11.HTTP hidden field manipulation;

1.7.1.1.111.12.HTTP request smuggling;

1.7.1.1.111.13.HTTP Response Splitting;

1.7.1.1.111.14.Malicious Robots;

1.7.1.1.111.15.Parameter Tampering;

1.7.1.1.111.16.Remote File Inclusion Attacks;

1.7.1.1.111.17.Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI);

1.7.1.1.111.18.Session Hijacking;

1.7.1.1.111.19.SQL Injection;

1.7.1.1.111.20.Web Scraping;

1.7.1.1.111.21.Web server software and operating system attacks;

1.7.1.1.111.22.Web Services (XML) attacks;

1.7.1.1.112. Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

1.7.1.1.113. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:

1.7.1.1.113.1. Assinatura de ataque;

1.7.1.1.113.2. Código de response;

1.7.1.1.113.3. Conteúdo da cookie;

1.7.1.1.113.4. Conteúdo do cabeçalho;

1.7.1.1.113.5. Conteúdo do payload;

1.7.1.1.113.6. Hostname;

1.7.1.1.113.7. IP de origem;

1.7.1.1.113.8. Método HTTP;

1.7.1.1.113.9. Número de ocorrências em determinado intervalo de tempo;

1.7.1.1.113.10.Parâmetro;

1.7.1.1.113.11.User-agent (navegador);

1.7.1.1.114. Permitir a criação de assinaturas de ataques.

1.7.1.1.115. Reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:

1.7.1.1.115.1. Ataques de negação de serviços automatizados;

1.7.1.1.115.2. Worms e vulnerabilidades conhecidas;

1.7.1.1.115.3. Requests em objetos restritos;

1.7.1.1.116. Deve proteger contra ataques SSRF (Server Side RequestForgery);

1.7.1.1.117. A solução oferecida deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra.

1.7.1.1.118. Deve possuir um conjunto de assinaturas para cada tipo de tecnologia bem definidos e agrupados. Portanto permitindo selecionar as tecnologias da aplicação (Apache, PHP, Linux, SQL, etc) para automaticamente selecionar o conjunto de assinaturas que se aplica as mesmas;

1.7.1.1.119. Ao atualizar ou adicionar uma nova assinatura, a solução deve automaticamente colocar essa assinatura em modo “staging” para evitar falsos positivos e não bloquear tráfego válido. Depois de um período a mesma deve automaticamente entrar em modo de bloqueio;

1.7.1.1.120. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (File Types);

1.7.1.1.121. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP;

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

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

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

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

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

1.7.1.1.125.2. CAPTCHA para suspeitos que ultrapassarem os thresholds;

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

1.7.1.1.126. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego, análise de dados e Machine Learning, com o stress do servidor de aplicação para determinar uma condição de DDoS;

1.7.1.1.127. Aprender o comportamento da aplicação:

1.7.1.1.127.1. Campos, valores, cookies e URLs;

1.7.1.1.128. Políticas sugeridas somente devem ser aplicadas após um período configurável;

1.7.1.1.129. Inspecionar e monitorar até a camada de aplicação, todo tráfego de dados HTTP, incluindo cabeçalhos, campos de formulários e conteúdo, além de inspecionar os requests e responses;

1.7.1.1.130. Realizar as checagens em todos os tipos de entrada de dados, como URLs, formulários, cookies, campos ocultos e parâmetros, consultas (query), métodos HTTP, elementos XML e ações SOAP;

1.7.1.1.131. Proteger contra mensagens XML e SOAP malformadas;

1.7.1.1.132. Utilizar o campo HTTP X-Forwarded-For sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT;

1.7.1.1.133. Remover as mensagens de erro do conteúdo que será enviado aos usuários;

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

1.7.1.1.135. Deverá permitir o cadastro de robôs que podem acessar a aplicação;

1.7.1.1.136. Deverá implementar proteção ao JSON (JavaScript Object Notation);

1.7.1.1.137. Implementar a segurança de web services, através dos seguintes métodos:

1.7.1.1.137.1. Criptografar/Decriptografar partes das mensagens SOAP;

1.7.1.1.137.2. Assinar digitalmente partes das mensagens SOAP;

1.7.1.1.137.3. Verificação de partes das mensagens SOAP;

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

1.7.1.1.139. Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;

1.7.1.1.140. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário. Deve proteger esses dados criptografados de malwares e keyloggers;

1.7.1.1.141. Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos. Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados;

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

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

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

1.7.1.1.145. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:

1.7.1.1.145.1. Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade.

1.7.1.1.146. Deverá permitir o agendamento de relatórios a serem entregues por email;

1.7.1.1.147. Emitir os seguintes relatórios gráficos dos alterar por:

1.7.1.1.147.1. Política de segurança;

1.7.1.1.147.2. Tipos de ataques;

1.7.1.1.147.3. Violações;

1.7.1.1.147.4. URL que foram atacadas;

1.7.1.1.147.5. Endereços IP de origem;

1.7.1.1.147.6. localização geográfica dos endereços IPs de origem;

1.7.1.1.147.7. Severidade;

1.7.1.1.147.8. Código de resposta;

1.7.1.1.147.9. Métodos;

1.7.1.1.147.10.Protocolos;

1.7.1.1.147.11.Sessão;

1.7.1.1.148. Permitir a seleção de período para emissão dos relatórios,

1.7.1.1.149. Permitir a geração das seguintes informações, por período:

1.7.1.1.149.1. Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

1.7.1.1.149.2. Informações estatísticas de quantidade de conexões completadas e bloqueadas;

1.7.1.1.149.3. Informações estatísticas de fluxo de tráfego;

1.7.1.1.149.4. Informações estatísticas de quantidade de sessões ou conexões;

1.7.1.1.150. Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: HTTP e HTTPS;

1.7.1.1.151. Deve possuir capacidade para definir que todo tráfego seja tunelado e permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento

1.7.1.1.152. Deve possuir capacidade para definir servidor virtual em HTTPS com perfil cliente SSL/TLS padrão e redirecionar tráfego HTTP para HTTPS para um determinado servidor virtual;

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

1.7.1.1.154. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado

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

1.7.1.1.155.1. SSL session cache Timeout;

1.7.1.1.155.2. Session Ticket;

1.7.1.1.155.3. OCSP (Online Certificate Status Protocol) Stapling;

1.7.1.1.155.4. Dynamic Record Sizing;

1.7.1.1.155.5. ALPN (Application Layer Protocol Negotiation);

1.7.1.1.155.6. Perfect Forward Secrecy;

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

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

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

1.7.1.1.156.3. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;

1.7.1.1.156.4. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS;

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

1.7.1.1.157. Deve possibilitar a customização da interface gráfica da página de login e mensagens de apresentação ao usuário de acordo com o grupo que pertença;

1.7.1.1.158. A solução deve oferecer ferramenta de Portal de Acesso de Usuários que permita que usuários acessem aplicações internas a partir de rede externas, implementando as funcionalidades de Single Sign-on e VPN-SSL, com os seguintes recursos:

1.7.1.1.158.1. modo “Túnel por aplicação” onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitido outro tipo de tráfego dentro do mesmo túnel;

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

1.7.1.1.158.3. modo “Network”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna;

1.7.1.1.158.4. Ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação, fazendo cache das credenciais do usuário e utilizar a credencial correta para cada sistema;

1.7.1.1.159. Deverá ser capaz de autenticar usuários em bases de dados LDAP, Radius, Tacacs+, Kerberos e RSA SecurID;

1.7.1.1.160. Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware ou one-time passcode (OTP); Deve possuir capacidade para realizar proxy reverso com a finalidade de omitir a URI real, promovendo assim o acesso seguro as aplicações web internas;

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

1.7.1.1.162. Deve possuir capacidade para realizar verificações e validações no dispositivo do cliente antes de conceder acesso tais como versão do sistema operacional, anti-vírus instalado, certificados digitais instalados na máquina, firewall ativado;

1.7.1.1.163. Melhora da disponibilidade das aplicações através do balanceamento da entrada de tráfego deve possuir, ao menos, as seguintes características:

1.7.1.1.163.1.1. DNS autoritativo;

1.7.1.1.163.1.2. DNS secundário;

1.7.1.1.163.1.3. DNS resolver;

1.7.1.1.163.1.4. DNS cache;

1.7.1.1.163.1.5. Balanceamento de DNS servers;

1.7.1.1.163.1.6. DNSSec;

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

1.7.1.1.165. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;

1.7.1.1.166. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT

1.7.1.1.167. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;

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

1.7.1.1.169. Deve prover as respostas a queries DNS da própria RAM CACHE

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

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

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

1.7.1.1.173. Suportar pelo menos os seguintes algoritmos de balanceamento:

1.7.1.1.173.1. Round Robin;

1.7.1.1.173.2. Global Availability;

1.7.1.1.173.3. Ratio;

1.7.1.1.173.4. LDNS Persist;

1.7.1.1.173.5. Geografia;

1.7.1.1.173.6. Disponibilidade da Aplicação;

1.7.1.1.173.7. Capacidade do Virtual Server;

1.7.1.1.173.8. Least Connections;

1.7.1.1.173.9. Pacotes por segundo;

1.7.1.1.173.10.Round trip time;

1.7.1.1.173.11.Hops;

1.7.1.1.173.12.Packet Completion Rate;

1.7.1.1.173.13.QoS definido pelo usuário;

1.7.1.1.173.14.Kilobytes per Second;

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

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

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

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

1.7.1.1.177.1. Usar o ECS para tomar decisões baseado em topologia (Subnets)

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

1.7.1.1.178. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver (suporte ECS).

1.7.1.1.179. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

1.7.1.1.180. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);

1.7.1.1.181. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;

1.7.1.1.182. Permitir o balanceamento de aplicações em um pool de servidores, independentemente do hardware, sistema operacional e tipo de aplicação;

1.7.1.1.183. Suportar os seguintes métodos de balanceamento:

1.7.1.1.183.1. Round Robin;

1.7.1.1.183.2. Least Connection;

1.7.1.1.183.3. Por peso.

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

1.7.1.1.183.5. Weighted Percentage dinâmico (baseado no número de conexões);

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

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

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

1.7.1.1.185.1. Por cookie;

1.7.1.1.185.2. Endereço de origem;

1.7.1.1.185.3. Sessão SSL;

1.7.1.1.185.4. Análise da URL acessada;

1.7.1.1.185.5. Através de qualquer parâmetro do cabeçalho HTTP;

1.7.1.1.185.6. Através da análise do MS Terminal Services Session (MSRDP)

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

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

1.7.1.1.186. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:

1.7.1.1.186.1. ICMP, TCP, HTTP, HTTPs;

1.7.1.1.186.2. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;

1.7.1.1.187. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor;

1.7.1.1.188. Realizar Network Address Translation (NAT);

1.7.1.1.189. Realizar proteção contra syn flood;

1.7.1.1.190. Realizar as proteções de cabeçalho: X-Frame-Options, X-XSS-Protection, X-Content- Type- Options

1.7.1.1.191. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;

1.7.1.1.192. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.

1.7.1.1.192.1. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.

1.7.1.1.192.2. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.

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

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

1.7.1.1.195. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;

1.7.1.1.196. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;

1.7.1.1.197. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

1.7.1.1.198. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;

1.7.1.1.199. Realizar Network Address Translation (NAT);

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

1.7.1.1.201. Realizar Proteção contra Syn flood;

1.7.1.1.202. Realizar Limpeza de cabeçalho HTTP;

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

1.7.1.1.204. Deve ser possível enviar, pelo menos, as seguintes informações via LLDP:

1.7.1.1.205. Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size;

1.7.1.1.206. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

1.7.1.1.207. Deve ser capaz de realizar DHCP relay;

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

1.7.1.1.208.1. Tempo de resposta da aplicação;

1.7.1.1.208.2. Latência;

1.7.1.1.208.3. Conexões para conjunto de servidores, servidores individuais;

1.7.1.1.208.4. Por URL;

1.7.1.1.209. A solução deve ter suporte a TLS 1.3;

1.7.1.1.210. A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas:

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

1.7.1.1.210.2. Deve possuir, pelo menos, as seguintes categorias de endereços IP: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing Proxy, Anonymous Proxy

1.7.1.1.211. A solução deve prover um serviço de campanhas de ameaças Web. Esse serviço deve prover atualizações dinâmicas de regras bem especificas de acordo com as últimas ameaças identificadas por um serviço de especialistas de segurança.

1.7.1.1.212. As atualizações desse serviço devem ser constantes e o nível de falso positivo muito baixo.

1.7.1.1.213. Deve prover inteligência para identificar e mitigar ataques sofisticados com alta precisão.

1.7.1.1.214. Deve usar Metadados para determinar requisições e intenções maliciosas e bloquear ameaças sem precisar de um ciclo de aprendizagem.

1.7.2. Requisitos técnicos - item 2

1.7.2.1. Especificação técnica mínima

1.7.2.1.1. Implantação: os serviços de instalação física, lógica deverão ser executados pela CONTRATADA e seguirão as fases de abertura do projeto, fase de planejamento, fase de execução e fase de documentação conforme estão detalhadas a seguir.

1.7.2.1.1.1. Fase de abertura:

a.)Validar e Homologar escopo do projeto;

b) Validar objetivos e premissas do projeto;

c) Validar riscos e restrições do projeto;

d) Identificar e validar os requisitos do projeto.

1.7.2.1.1.2. Fase de planejamento:

a) Elaborar plano de projeto;

b) Definir as pessoas envolvidas por parte da CONTRATANTE no projeto;

c) Reunir as equipes da CONTRATADA e CONTRATANTE;

d) Apresentação do cronograma do projeto com os prazos e responsabilidades;

e) Verificar os pré-requisitos do projeto;

f) Apresentar plano do projeto para a homologação por parte da CONTRATANTE.

1.7.2.1.1.3. Fase de execução: O serviço de instalação consiste na colocação do(s) equipamento(s) em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da CONTRATANTE e deve contemplar, no mínimo, o seguinte:

a) Instalação e configuração realizada de acordo com as recomendações do fabricante (recommended settings);

b) A CONTRATADA deverá efetuar a instalação do appliance virtual ou físico (conforme item solicitado) na infraestrutura indicada pelo CONTRATANTE, onde a configuração realizada deverá estar em conformidade com as recomendações do fabricante (recommended settings);

c) Conexão e configuração de todos os equipamentos e/ou componentes da solução da rede do CONTRATANTE, inclusive configuração de VLANs e interfaces virtuais, se for o caso;

d) Atualização de softwares, firmwares e drives que compõem a solução;

e) A CONTRATADA deverá fornecer, quando for o caso, todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução entregue;

f) Aplicação das licenças necessárias à solução entregue;

g) Testes da solução, incluindo testes de failover;

h) Documentação do ambiente configurado e instalado.

1.7.2.1.2. A CONTRATADA será integralmente responsável pela interligação das interfaces com os switches de núcleo da rede da CONTRATANTE.

1.7.2.1.3.Todas as informações necessárias à implantação, como topologia de rede, VLANs, endereçamento IP, portas de Swtichs que devem ser utilizadas e outras necessárias à perfeita configuração, interligação e funcionamento da solução serão fornecidas pelo CONTRATANTE.

1.7.2.1.4. A instalação física do equipamento será realizada pela Contratada, com acompanhamento de uma equipe destacada pela CONTRATANTE.

1.7.2.1.5. A contratada deverá providenciar um profissional certificado pelo fabricante na solução para garantir a conformidade da instalação e a configuração dos equipamentos e softwares que compõem a solução.

1.7.2.1.6. A instalação, configuração e testes do equipamento deverá ser feita com o acompanhamento de técnicos da CONTRATANTE, visando o repasse de conhecimento e observados os padrões de gerenciamento de manutenção e segurança da CONTRATANTE.

1.7.2.1.7 O equipamento ou appliance virtual deverá estar com todas as funcionalidades e recursos de hardware e software solicitados disponíveis e configurados.

1.7.2.1.8. A instalação e a configuração do equipamento ou appliance virtual deverão ocorrer preferencialmente em dias úteis, em horário comercial, ficando a cargo da CONTRATANTE a definição dos horários para configuração do equipamento em produção. Atividades a serem realizadas fora deste horário, assim como a necessidade de interrupção de serviços em produção, estarão sujeitas à aprovação prévia da equipe técnica da CONTRATANTE

1.7.3. Requisitos técnicos - item 3

1.7.3.1. Especificação técnica mínima

1.7.3.1.1. Trata-se do serviço de treinamento com profissional certificado pelo fabricante da solução, cujo escopo do treinamento cubra conceitos de configuração, operação, administração, gerência, otimização, resolução de problemas e gestão de todos os componentes da solução de forma que o(s) servidor(es) capacitado(s) possam colocar os equipamentos e softwares em produção, bem como planejar mudanças de configuração no ambiente.

a) O treinamento deverá oferecer carga horária total de no mínimo 20(vinte) horas.

b) Serão aceitos apenas treinamentos nas modalidades presencial ou online ao vivo (EAD), podendo os treinamentos online ao vivo serem gravados, a critério da CONTRATANTE.

c) A CONTRATADA deve prover capacitação técnica em turma com no mínimo 4 (cinco) e no máximo 6 (seis) participantes.

d) Se o treinamento for ofertado na modalidade EAD, deverá respeitar o limite de 4 (quatro) horas por dia.

e) O treinamento for ofertado na modalidade na modalidade presencial, deverá ser ministrado em local fornecido pela Contratada, de segunda a sexta-feira, das 8:00 às 12:00, das 14:00 às 18:00 ou das 8:00 às 18:00.

f) As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA.

1.7.3.1.2. O treinamento poderá ser composto de mais de 1(um) módulo, que deverão ser discriminados na proposta da licitante.

1.7.3.1.3. A licitante proponente deverá entregar, na fase de habilitação, uma declaração afirmando que oferta o treinamento oficial do fabricante da solução e que a ementa e todo o material oferecido é aprovado pelo fabricante do equipamento, bem como, indicar na proposta o calendário contendo as datas e as localidades de realização do Treinamento.

1.7.3.1.4. A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar que o(s) treinamento(s) ofertados atendem os requisitos indicados no item

1.7.3.1.5. É facultado ao STM a realização de diligências e verificação da autenticidade da declaração e demais documentos comprobatórios.

1.7.3.1.6. O STM 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.

1.7.3.1.7. O treinamento deverá ser ministrado em data oportuna a ser informada à fiscalização após ou antes da instalação dos equipamentos, ficando a critério da administração e baseando-se no calendário a ser fornecido pela contratada.

1.7.3.1.8. 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.

1.7.3.1.9. O treinamento deverá ser ministrado por profissionais certificados pelo fabricante, cuja comprovação deverá ser encaminhada na assinatura do Contrato.

1.7.3.1.10. A contratada deverá fornecer material didático individual que abranja todo o conteúdo do(s) curso(s). Todo o material didático oferecido pela Contratada para realização do treinamento oficial do fabricante deverá ser oficial do fabricante da solução, ser de primeiro uso, atualizado e poderá estar em inglês ou português.

1.7.3.1.11. O treinamento deve ser ministrado em português do Brasil. O material do treinamento deve ser, preferencialmente, impresso e em português. Caso não exista material oficial do produto em língua portuguesa e impresso, será aceito material em inglês e na modalidade digital.

1.7.3.1.12. O treinamento deverá ocorrer em centro especializado para este fim, com acesso ao laboratório prático virtual, fornecido pela contratada, para configuração e execução de exercícios práticos.

1.7.3.1.12.1. No ambiente de treinamento, os servidores indicados pelo CONTRATANTE devem ter acesso em ambiente de laboratório a todos os produtos ofertados (ou similares) para realização da capacitação.

1.7.3.1.13. Os custos com deslocamento da equipe técnica do Superior Tribunal Militar para a cidade onde se realizará o treinamento (Centros Especializados de Treinamento) serão de responsabilidade da CONTRATADA.

1.7.3.1.14. A Contratada deverá emitir para o servidor participante, sem ônus para o Superior Tribunal Militar e no prazo máximo de até 10 (dez) dias úteis após o término do treinamento oficial do fabricante, o certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia desse certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento.

1.7.3.1.14.1. O certificado de conclusão do curso deverá ser emitido pelo fabricante ou pela empresa a ser contratada, ou ainda pela responsável legal pelo treinamento se terceirizado.

1.7.3.1.15. A ausência do servidor ao treinamento é de responsabilidade do Superior Tribunal Militar, cabendo a contratada informar no certificado a carga horária e assiduidade do servidor.

1.7.3.1.16. O treinamento ofertado deve seguir os modelos padrão de capacitação disponíveis no mercado naquilo que couber.

1.7.3.1.17. Não serão aceitos treinamentos não oficiais ou cujo conteúdo ministrado não abranja a utilização da solução para o fim a que se destina, bem ainda, aqueles cujos certificados não forem emitidos no prazo máximo de 5 dias contados da conclusão da capacitação.

a) A não aceitação da capacitação implicará no não pagamento dos serviços realizados.

b) A empresa a ser contratada deverá emitir certificados de participação contendo a exata carga horária do treinamento e a participação do treinando.

1.7.3.1.18. A Contratada deverá aplicar o Formulário de Satisfação, conforme modelo constante no Anexo A deste Termo de Referência.

a) No Formulário, será utilizada escala de até 5 (cinco) pontos para cada quesito. No mínimo 70% dos participantes deverão atribuir grau igual ou superior a 3 (três), para o item avaliado ser considerado proveitoso.

b) O resultado da Avaliação de Instrutor/Tutor será utilizado como critério de aceitação do treinamento oficial do fabricante, devendo ser considerado pela amostra de participantes como “proveitoso” para no mínimo 6 (seis) dos 10 (dez) itens avaliados;

c) Caso o resultado da Avaliação de Instrutor/Tutor seja considerado “não proveitoso”, o treinamento oficial do fabricante fornecido será considerado não aceito;

d) Na hipótese de não aceitação, a CONTRATADA deve oferecer outro treinamento oficial do fabricante, com a mesma carga horária, com outro instrutor, sem qualquer ônus para o CONTRATANTE:

e) Na hipótese de o resultado do segundo treinamento oficial do fabricante ser “não proveitoso”, o objeto será considerado não aceito, aplicando-se as sanções previstas contratualmente.

1.7.4. Requisitos técnicos - item 4

1.7.4.1. Especificação técnica mínima

1.7.4.1.1. A Contratada deverá fornecer garantia técnica de pelo menos 60 (sessenta) meses para a solução, contados a partir da data de emissão do Termo de Recebimento Definitivo relativo à fase de instalação;

1.7.4.1.2. 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 equipamentos e aplicativos permanentemente em perfeitas condições de funcionamento para a finalidade a que se destinam;

1.7.4.1.3. 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;

1.7.4.1.4. 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 48 (quarenta e oito) horas a partir de notificação do CONTRATANTE;

1.7.4.1.5. 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;

1.7.4.1.6. Suporte Técnico durante o período de Garantia Técnica:

1.7.4.1.6.1. Durante o período de garantia técnica de 60 (sessenta) 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;

1.7.4.1.6.2. 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;

1.7.4.1.6.3. 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;

1.7.4.1.7. A contratada deverá entregar no protocolo do CONTRATANTE, mensalmente, até o 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:

1.7.4.1.7.1. 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;

1.7.4.1.7.2. Cada chamado técnico aberto será avaliado individualmente pelo Gestor do Contrato;

1.7.4.1.7.3. 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;

1.7.4.1.7.4. 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.

1.7.4.1.8. A Contratada deverá fornecer versão atualizada do manual e demais documentos técnicos sempre que houver atualização nos manuais, nos softwares ou nos equipamentos da solução.

1.7.4.1.9. 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 equipamentos, desde que tal iniciativa não implique em danos físicos e lógicos aos equipamentos, sem que isto possa ser usado como pretexto pela Contratada para se desobrigar do suporte da solução.

1.7.4.1.10. A Contratada deverá garantir pleno funcionamento dos equipamentos 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.

1.7.4.1.11. A Contratada deverá dispor de serviço de esclarecimento de dúvidas relativas à utilização dos equipamentos e de abertura de chamado técnico por e-mail ou por telefone 0800 (gratuito), ou telefone local em Brasília por todo o período da garantia técnica.

1.7.4.1.12. A Contratada deverá garantir, sem quaisquer custos adicionais, as atualizações havidas nos equipamentos nas versões de software e firmware, inclusive releases, pelo prazo de vigência da garantia;

1.7.4.1.13. O serviço de garantia técnica deverá permitir o acesso do CONTRATANTE à base de dados de conhecimento do fabricante dos equipamentos, 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 equipamentos.

1.7.4.1.14. 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.

1.7.4.1.15. Quando a garantia técnica for acionada, o atendimento deverá ser iniciado imediatamente, independente do meio utilizado. A cada abertura de chamada, a Contratada deverá fornecer ao CONTRATANTE um código identificador único para acompanhamento.

1.7.4.1.16. 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

1.8. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

1.8.1. A estimativa de custo total apresentado neste estudo técnico para o período de 60 (sessenta) meses, é de aproximadamente R$ 4.031.879,70 (quatro milhões, trinta e um mil, oitocentos e setenta e nove reais e setenta centavos).

	ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QNTD.	Valor TOTAL:
GRUPO 1	1	Solução de Proteção de Aplicações e Balanceamento de Carga (WAF) com Suporte Especializado e garantia pelo período de 60 (sessenta) meses.	UN	2	R$ 3.099.744
	2	Serviço de Implantação e configuração da solução.	UN	1	R$ 92.014,28
	3	Treinamento	UN	6	R$ 139621,42
	4	Suporte Especializado pelo período de 60 (sessenta) meses		60	R$ 700.500,00
	Média Total				R$ 4.031.879,70

2. SUSTENTAÇÃO DO CONTRATO

2.1 Adequação do Ambiente

Para execução do objeto pretendido é necessário dispor de infraestrutura física para instalação dos equipamentos pretendidos, como cabeamento, energia elétrica e espaço em rack. Essa infraestrutura já está disponível no local de instalação dos equipamentos, em todas as localidades do STM.

2.2 Recursos Materiais e Humanos

Em relação aos recursos humanos, o objeto a ser contratado não impõe necessidades especiais de pessoal, além dos já disponíveis no STM.

Os recursos materiais necessários para o pleno funcionamento da solução pretendida deverão ser fornecidos pela Contratada.

2.3. Descontinuidade do Fornecimento

Caso o fornecedor contratado entregue parcialmente ou não consiga entregar a solução completa ora pretendida, poder-se-á proceder com a contratação de outra empresa do mercado privado.

Em caso de descontinuidade da prestação do serviço durante a vigência do contrato, poder-se-á aplicar as cláusulas contratuais estipuladas para este caso, e proceder com nova contratação junto a outro fornecedor.

2.4 Transição Contratual e encerramento do contrato

Em caso de insucesso da contratação ora pretendida, e havendo situação inesperada ou repentina de transição ou de encerramento do contrato, algumas medidas poderão ser adotadas pelo STM, como as já mencionadas anteriormente no item 2.2 destes Estudos Preliminares.

Apesar de remota, pelos conhecimentos e informações que a COTEC possui no momento, a possibilidade de descontinuidade desse tipo de solução no mercado poderá existir. Todavia, há no mercado privado várias soluções que poderão fornecer o objeto dessa contratação.

3. ESTRATÉGIA PARA A CONTRATAÇÃO

3.1 Natureza do Objeto

O objeto a ser contratado possui características comuns e usuais encontradas atualmente no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos no Termo de Referência.

Ainda, trata-se de objeto de natureza continuada, visto que se destina ao atendimento de uma necessidade perene e essencial, já que a sua interrupção irá comprometer as atividades do STM

3.2 Parcelamento do Objeto.

Considerando o disposto no §1º do artigo 23 da lei 8666/93 onde as obras, serviços e compras efetuadas pela Administração serão divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis. Os itens especificados de cada grupo estão fortemente integrados entre si, sendo necessária sua execução por uma mesma empresa para que não se configure conflito de competências quando da solicitação e/ou cobrança das atividades realizadas, além de reduzir a complexidade da gestão do contrato, reduzir seus custos de administração e reduzir os riscos operacionais e conflitos. Desta forma, os itens objeto do presente termo de referência serão agrupados

Dessa forma, a adjudicação será integralmente realizada a um único fornecedor para o grupo pelo menor preço global.

3.3 Adjudicação do Objeto

Sugere-se que a adjudicação seja realizada de forma global, ou seja, todos os itens que comporão o objeto de contratação deverão ser adjudicados a um único fornecedor e agrupados em um único grupo, pois todos os bens e serviços estão intrinsecamente relacionados, sendo declarado vencedor o licitante que apresentar a proposta com o menor valor global do grupo. Tal organização permite ganhos quanto à instalação, configuração e operacionalização de toda a solução.

3.4 Modalidade e Tipo de Licitação

Por se tratar de contratação de bens e serviços comuns, nos termos do parágrafo único do art. 1º da Lei nº 10.520/02, o certame licitatório será realizado por meio de Sistema de Registro de Preços, na modalidade Pregão, em sua forma eletrônica, do tipo menor preço global.

Como a aquisição pretendida será em grupo e a a contratação não se dará logo após a licitação, tendo em vista que a instalação do equipamento em cluster será por etapas, sugerimos a aplicação da modalidade de Sistema de Registro de Preços.

Por se tratar de bens usuais no mercado e passíveis de serem definidos de forma objetiva, o objeto em questão se enquadra na definição de bens e serviços comuns

3.5 Classificação e Indicação orçamentária

Entende-se que a classificação do objeto se insere em despesas correntes, pois trata-se de despesas de custeio de manutenção das atividades dos órgãos da administração pública.

3.6 Vigência contratual

3.6.1. O prazo de execução referente itens 1 e 2 será de até 60 dias, após o recebimento da nota de empenho.

3.6.2. A vigência do contrato referente ao item 3 será de 12 meses, a contar de sua assinatura

3.6.3. A vigência do contrato referente ao item 4 será de 60 meses, a contar de sua assinatura

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		
Integrante Técnico	Integrante Demandante	Integrante Administrativo
Marcio Coelho Marques	**Wilson Marques de Souza Filho**	**Luis Gustavo Costa Reis**

VALIDAÇÃO ESTUDO TÉCNICO PRELIMINAR
Autoridade da Área Demandante **IANNE CARVALHO BARROS** Diretor de Tecnologia da Informação

Documento assinado eletronicamente por **WILSON MARQUES DE SOUZA FILHO**, **COORDENADOR DE TECNOLOGIA**, em 12/06/2023, às 18:04 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **IANNE CARVALHO BARROS**, **DIRETOR DE TECNOLOGIA DA INFORMAÇÃO**, em 13/06/2023, às 11:03 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUIS GUSTAVO COSTA REIS**, **INTEGRANTE ADMINISTRATIVO**, em 13/06/2023, às 13:36 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCIO COELHO MARQUES**, **ANALISTA JUDICIÁRIA - Apoio Especializado - Análise de Sistemas**, em 13/06/2023, às 14:30 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **3249005** e o código CRC **2F6F59C8**.