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

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de empresa para fornecimento 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, **pelo Sistema de Registro de Preços.**

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

A Justiça Militar da União (JMU) passou a integrar o Poder Judiciário a partir da Constituição de 1934 e seus julgamentos seguem a mesma sistemática do Judiciário Brasileiro.

Na condição de serviço público, a JMU submete-se também ao Princípio da Continuidade, também conhecido como Princípio da Permanência, o qual veda a estas instituições a opção pela interrupção de suas atividades em face dos potenciais prejuízos para o cidadão e para a sociedade. Neste sentido, a Constituição Federal de 1988 em seu § 6º do artigo 37, determina que "[...] pessoas jurídicas de direito público [...] responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa."

Considerando o princípio da continuidade, e na esteira da invasão sofrida pelo Superior Tribunal de Justiça (STJ) em novembro de 2020, o Conselho Nacional de Justiça, órgão responsável pelo controle da atuação administrativa e financeira dos tribunais, instituiu a Resolução nº 396/2021 para consolidar a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). O documento, que abrange todos os Tribunais Nacionais, determinam ações para elevar o nível da segurança cibernética do ecossistema digital do Poder Judiciário brasileiro. Entre outras medidas, a Resolução CNJ nº 396/2021 tornam obrigatórias ações dos Tribunais no sentido de remover ou mitigar riscos de que ataques como o perpetrado contra o STJ, não voltem a prejudicar a prestação jurisdicional ao ponto de interromper suas atividades.

O STM possui atualmente diversos sistemas *web*, tanto para uso dos servidores e colaboradores, disponíveis de forma interna como SRH, Ponto Eletrônico; e outros sistemas utilizados interna e externamente como SEI, eProc, GEAFIN, SIPOC, entre outros. Esses sistemas são protegidos por uma série de soluções que fazem parte da infraestrutura do Datacenter do STM, porém com a evolução constante dos métodos de ataques que tem como finalidade a extração, modificação e até a indisponibilidade dos dados, faz-se necessária a utilização de ferramentas específicas para a proteção dos dados expostos na *internet.*

No passado, a principal solução de tecnologia para segurança de aplicações web era de responsabilidade do *firewall*. A tecnologia evoluiu e foi criado o *Web Application Firewall (WAF)* para análise e proteção contra ameaças cibernéticas que estão além da capacidade dos *firewalls* tradicionais, criando uma barreira entre serviço baseado na *web* e os principais ataques.

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.

Conclui-se, assim, a necessidade desta nova camada de proteção, que tenha a capacidade de tomar ações rápidas para conter ameaças com rapidez e eficiência e potencializar o desempenho para aplicações *web* do STM

A unidade demandante, COTEC, buscando o aprimoramento da segurança das informações internas e das de propriedade dos cidadãos sob a custódia do STM, tem a necessidade de contratar uma solução de *Web Application Firewall* para analisar e proteger de ameaças que estão além da capacidade dos *firewalls* tradicionais, criando uma barreira entre serviço baseado na web e as principais ameaças.

3. OBJETIVOS A SEREM ALCANÇADOS POR MEIO DA CONTRATAÇÃO

3.1. Dentre os benefícios, destacam-se:

3.1.1. Garantir à disponibilidade da solução que fornece proteção contra ataques virtuais;

3.1.2. Alta disponibilidade e integridade do ambiente tecnológico deste Tribunal;

3.1.3. Manter as aplicações web mais seguras, com a implementação de regras personalizadas, minimizando os problemas relacionados, cite-se:

- Injeção de dados;
- Exposição de dados confidenciais;
- Quebra de sessão e gerenciamento de sessões;

3.1.4. Maturidade do processo de monitoramento, através da predefinição e personalização de gráficos de monitoramento e envio de notificações.

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

5. PARCELAMENTO DO OBJETO E ADJUDICAÇÃO

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.

6. ALINHAMENTO ENTRE A CONTRATAÇÃO DE FORNECIMENTO E O PLANEJAMENTO ESTRATÉGICO DA JMU

A análise, está em consonância com a necessidade de prover uma solução capaz de atender as demandas da JMU, de forma a atingir os objetivos propostos por este projeto, em especial possibilitar a realização de análises em tempo exíguo para tomadas de decisão, viabilizando inclusive emissão de relatórios gerenciais e ampliação do conhecimento sistêmico organizacional.

Objetivo: Fortalecer a governança e a segurança de dados e informações.

Estratégia: Compatibilizar a infraestrutura e as soluções de TIC às necessidades da JMU.

Iniciativa: Aperfeiçoar a gestão e a proteção de dados e informações.

7. ESTUDOS

Os Estudos Técnicos Preliminares (Documento de Oficialização da Demanda – DOD, a Análise de Viabilidade da Contratação, a Sustentação do Contrato, a Estratégia para a Contratação e a Análise de Riscos) foram realizados pela equipe de Planejamento de conforme determinado o art. 12, § 1º, da Resolução nº 182/13, do CNJ.

8. RELAÇÃO ENTRE A DEMANDA PREVISTA E OS SERVIÇOS A SEREM CONTRATADOS

8.1. 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; treinamento para capacitação técnica da equipe interna do Superior Tribunal Militar e suporte especializado pelo período de 60 (sessenta) meses.

	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.	MÊS	60

9. JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

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.

10. ESPECIFICAÇÃO TÉCNICA

10.1. Requisitos do Demandante

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.

10.2. 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.

10.2. 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

10.2.1 Requisitos técnicos - item 1

10.2.1.1. Especificação técnica mínima

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

10.2.1.1.2. 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.

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

10.2.1.1.4. 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.

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

10.2.1.1.6. 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;

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

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

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

10.2.1.1.10. 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;

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

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

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

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

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

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

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

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

10.2.1.1.19. Memória RAM mínima de 32 GB;

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

10.2.1.1.21. 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

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

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

10.2.1.1.24. 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.

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

10.2.1.1.26. 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.

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

10.2.1.1.28. 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.

10.2.1.1.29. 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;

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

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

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

10.2.1.1.33. Possuir suporte a IPv6;

10.2.1.1.34. 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;

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

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

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

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

10.2.1.1.39. O equipamento deverá permitir a sincronização das configurações:

10.2.1.1.39.1. De forma automática;

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

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

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

10.2.1.1.40.1.2. Utilizar uma rede exclusiva para o heartbeat.

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

10.2.1.1.42. 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.

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

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

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

10.2.1.1.46. 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.

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

10.2.1.1.48. Permitir acesso in-band via SSH

10.2.1.1.49. 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.

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

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

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

10.2.1.1.51. Manter internamente múltiplos arquivos de configurações do sistema;

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

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

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

10.2.1.1.55. Possuir Interface Gráfica via Web;

10.2.1.1.56. Possuir auto-complementação de comandos na CLI;

10.2.1.1.57. Possuir ajuda contextual;

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

10.2.1.1.59. A Solução deve ter suporte a sFlow;

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

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

10.2.1.1.62. 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;

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

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

10.2.1.1.65. Suportar a rollback de configuração e imagem;

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

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

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

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

10.2.1.1.70. Reinicialização do equipamento por comando na CLI;

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

10.2.1.1.72. Possuir traps SNMP;

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

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

10.2.1.1.75. Implementar Debugging: CLI via console e SSH;

10.2.1.1.76. Permite a criação de políticas diferenciadas por aplicação e por

URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

10.2.1.1.77. Permitir a criação de políticas diferenciadas por aplicação.

10.2.1.1.78. 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;

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

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

10.2.1.1.81. Permitir as seguintes opções de implementação:

10.2.1.1.82. Monitoramento (sem bloqueio);

10.2.1.1.83. Proxy (reverso e transparente).

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

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

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

10.2.1.1.87. 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;

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

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

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

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

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

10.2.1.1.92. 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;

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

10.2.1.1.94. Bloqueio com intermediação e interrupção da conexão;

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

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

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

10.2.1.1.98. 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;

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

10.2.1.1.99.1. Endereços IP que originaram os ataques;

10.2.1.1.99.2. Horário do ataque;

10.2.1.1.99.3. Nome do ataque;

10.2.1.1.99.4. Qual campo foi atacado;

10.2.1.1.99.5. Quantas vezes esse ataque foi realizado;

10.2.1.1.100. 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;

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

10.2.1.1.102. Identificar ataques baseados em:

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

10.2.1.1.102.2. Regras;

10.2.1.1.102.3. Perfis de utilização;

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

10.2.1.1.104. 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.

10.2.1.1.105. 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.

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

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

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

10.2.1.1.109. Detectar ataques do tipo força bruta em que:

10.2.1.1.109.1. O atacante solicita repetidamente o mesmo recurso;

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

10.2.1.1.109.3. São utilizados ataques automatizados de login.

10.2.1.1.110. Detectar ataques do tipo força bruta que explorem:

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

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

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

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

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

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

10.2.1.1.110.7. 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;

10.2.1.1.110.8. Possibilitar atualização de novas assinaturas para ataques conhecidos;

10.2.1.1.111. Apresentar proteção contra-ataques, como:

10.2.1.1.111.1. Brute Force Login;

10.2.1.1.111.2. Buffer Overflow;

10.2.1.1.111.3. Cookie Injection;

10.2.1.1.111.4. Cookie Poisoning;

10.2.1.1.111.5. Cross Site Request Forgery (CSRF);

10.2.1.1.111.6. Cross Site Scripting (XSS);

10.2.1.1.111.7. Server Side Request Forgery (SSRF)

10.2.1.1.111.8. Directory Traversal;

10.2.1.1.111.9. Forceful Browsing;

10.2.1.1.111.10.HTTP Denial of Service;

10.2.1.1.111.11.HTTP hidden field manipulation;

10.2.1.1.111.12.HTTP request smuggling;

10.2.1.1.111.13.HTTP Response Splitting;

10.2.1.1.111.14.Malicious Robots;

10.2.1.1.111.15.Parameter Tampering;

10.2.1.1.111.16.Remote File Inclusion Attacks;

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

10.2.1.1.111.18.Session Hijacking;

10.2.1.1.111.19.SQL Injection;

10.2.1.1.111.20.Web Scraping;

10.2.1.1.111.21.Web server software and operating system attacks;

10.2.1.1.111.22.Web Services (XML) attacks;

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

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

10.2.1.1.113.1. Assinatura de ataque;

10.2.1.1.113.2. Código de response;

10.2.1.1.113.3. Conteúdo da cookie;

10.2.1.1.113.4. Conteúdo do cabeçalho;

10.2.1.1.113.5. Conteúdo do payload;

10.2.1.1.113.6. Hostname;

10.2.1.1.113.7. IP de origem;

10.2.1.1.113.8. Método HTTP;

10.2.1.1.113.9. Número de ocorrências em determinado intervalo de tempo;

10.2.1.1.113.10.Parâmetro;

10.2.1.1.113.11.User-agent (navegador);

10.2.1.1.114. Permitir a criação de assinaturas de ataques.

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

10.2.1.1.115.1. Ataques de negação de serviços automatizados;

10.2.1.1.115.2. Worms e vulnerabilidades conhecidas;

10.2.1.1.115.3. Requests em objetos restritos;

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

10.2.1.1.117. 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.

10.2.1.1.118. 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;

10.2.1.1.119. 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;

10.2.1.1.120. Deve permitir que possa ser especificado na política os tipos de

arquivos que serão bloqueados (File Types);

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

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

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

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

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

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

10.2.1.1.125.2. CAPTCHA para suspeitos que ultrapassarem os thresholds;

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

10.2.1.1.126. 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;

10.2.1.1.127. Aprender o comportamento da aplicação:

10.2.1.1.127.1. Campos, valores, cookies e URLs;

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

10.2.1.1.129. 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;

10.2.1.1.130. 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;

10.2.1.1.131. Proteger contra mensagens XML e SOAP malformadas;

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

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

10.2.1.1.134. 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;

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

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

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

10.2.1.1.137.1. Criptografar/Decriptografar partes das mensagens SOAP;

10.2.1.1.137.2. Assinar digitalmente partes das mensagens SOAP;

10.2.1.1.137.3. Verificação de partes das mensagens SOAP;

10.2.1.1.138. 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;

10.2.1.1.139. 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;

10.2.1.1.140. 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;

10.2.1.1.141. 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;

10.2.1.1.142. 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;

10.2.1.1.143. 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;

10.2.1.1.144. 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.

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

10.2.1.1.145.1. 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.

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

10.2.1.1.147. Emitir os seguintes relatórios gráficos dos alterar por:

10.2.1.1.147.1. Política de segurança;

10.2.1.1.147.2. Tipos de ataques;

10.2.1.1.147.3. Violações;

10.2.1.1.147.4. URL que foram atacadas;

10.2.1.1.147.5. Endereços IP de origem;

10.2.1.1.147.6. localização geográfica dos endereços IPs de origem;

10.2.1.1.147.7. Severidade;

10.2.1.1.147.8. Código de resposta;

10.2.1.1.147.9. Métodos;

10.2.1.1.147.10.Protocolos;

10.2.1.1.147.11.Sessão;

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

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

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

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

10.2.1.1.149.3. Informações estatísticas de fluxo de tráfego;

10.2.1.1.149.4. Informações estatísticas de quantidade de sessões ou conexões;

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

10.2.1.1.151. 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

10.2.1.1.152. 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;

10.2.1.1.153. 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.

10.2.1.1.154. 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

10.2.1.1.155. 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:

10.2.1.1.155.1. SSL session cache Timeout;

10.2.1.1.155.2. Session Ticket;

10.2.1.1.155.3. OCSP (Online Certificate Status Protocol) Stapling;

10.2.1.1.155.4. Dynamic Record Sizing;

10.2.1.1.155.5. ALPN (Application Layer Protocol Negotiation);

10.2.1.1.155.6. Perfect Forward Secrecy;

10.2.1.1.156. 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:

10.2.1.1.156.1. 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;

10.2.1.1.156.2. 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;

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

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

10.2.1.1.156.5. 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.

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

10.2.1.1.158. 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:

10.2.1.1.158.1. 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;

10.2.1.1.158.2. 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;

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

10.2.1.1.158.4. 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;

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

10.2.1.1.160. 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;

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

10.2.1.1.162. 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;

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

10.2.1.1.163.1.1. DNS autoritativo;

10.2.1.1.163.1.2. DNS secundário;

10.2.1.1.163.1.3. DNS resolver;

10.2.1.1.163.1.4. DNS cache;

10.2.1.1.163.1.5. Balanceamento de DNS servers;

10.2.1.1.163.1.6. DNSSec;

10.2.1.1.164. 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;

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

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

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

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

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

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

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

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

10.2.1.1.173. Suportar pelo menos os seguintes algoritmos de balanceamento:

10.2.1.1.173.1. Round Robin;

10.2.1.1.173.2. Global Availability;

10.2.1.1.173.3. Ratio;

10.2.1.1.173.4. LDNS Persist;

10.2.1.1.173.5. Geografia;

10.2.1.1.173.6. Disponibilidade da Aplicação;

10.2.1.1.173.7. Capacidade do Virtual Server;

10.2.1.1.173.8. Least Connections;

10.2.1.1.173.9. Pacotes por segundo;

10.2.1.1.173.10.Round trip time;

10.2.1.1.173.11.Hops;

10.2.1.1.173.12.Packet Completion Rate;

10.2.1.1.173.13.QoS definido pelo usuário;

10.2.1.1.173.14.Kilobytes per Second;

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

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

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

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

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

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

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

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

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

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

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

10.2.1.1.183. Suportar os seguintes métodos de balanceamento:

10.2.1.1.183.1. Round Robin;

10.2.1.1.183.2. Least Connection;

10.2.1.1.183.3. Por peso.

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

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

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

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

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

10.2.1.1.185.1. Por cookie;

10.2.1.1.185.2. Endereço de origem;

10.2.1.1.185.3. Sessão SSL;

10.2.1.1.185.4. Análise da URL acessada;

10.2.1.1.185.5. Através de qualquer parâmetro do cabeçalho HTTP;

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

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

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

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

10.2.1.1.186.1. ICMP, TCP, HTTP, HTTPs;

10.2.1.1.186.2. 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;

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

10.2.1.1.188. Realizar Network Address Translation (NAT);

10.2.1.1.189. Realizar proteção contra syn flood;

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

10.2.1.1.191. 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;

10.2.1.1.192. 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.

10.2.1.1.192.1. 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.

10.2.1.1.192.2. 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.

10.2.1.1.193. 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

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

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

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

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

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

10.2.1.1.199. Realizar Network Address Translation (NAT);

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

10.2.1.1.201. Realizar Proteção contra Syn flood;

10.2.1.1.202. Realizar Limpeza de cabeçalho HTTP;

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

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

10.2.1.1.205. 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;

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

10.2.1.1.207. Deve ser capaz de realizar DHCP relay;

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

10.2.1.1.208.1. Tempo de resposta da aplicação;

10.2.1.1.208.2. Latência;

10.2.1.1.208.3. Conexões para conjunto de servidores, servidores individuais;

10.2.1.1.208.4. Por URL;

10.2.1.1.209. A solução deve ter suporte a TLS 1.3;

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

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

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

10.2.1.1.211. 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.

10.2.1.1.212. As atualizações desse serviço devem ser constantes e o nível de

falso positivo muito baixo.

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

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

10.2.2. Requisitos técnicos - item 2

10.2.2.1. Especificação técnica mínima

10.2.2.1.1. 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.

10.2.2.1.1.1. 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.

10.2.2.1.1.2. 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.

10.2.2.1.1.3. 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.

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

10.2.2.1.3.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.

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

10.2.2.1.5. 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.

10.2.2.1.6. 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.

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

10.2.2.1.8. 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

10.2.3. Requisitos técnicos - item 3

10.2.3.1. Especificação técnica mínima

10.2.3.1.1. 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.

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

10.2.3.1.3. A licitante proponente deverá entregar 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.

10.2.3.1.4. 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

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

10.2.3.1.6. 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.

10.2.3.1.7. 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.

10.2.3.1.8. 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.

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

10.2.3.1.10. 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.

10.2.3.1.11. 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.

10.2.3.1.12. 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.

10.2.3.1.12.1. 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.

10.2.3.1.13. 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.

10.2.3.1.14. 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.

10.2.3.1.14.1. 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.

10.2.3.1.15. 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.

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

10.2.3.1.17. 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.

10.2.4. Requisitos técnicos - item 4

10.2.4.1. Especificação técnica mínima

10.2.4.1.1. 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;

10.2.4.1.2. 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;

10.2.4.1.3. 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;

10.2.4.1.4. 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;

10.2.4.1.5. 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;

10.2.4.1.6. Suporte Técnico durante o período de Garantia Técnica:

10.2.4.1.6.1. 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;

10.2.4.1.6.2. 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;

10.2.4.1.6.3. 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;

10.2.4.1.7. 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:

10.2.4.1.7.1. 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;

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

10.2.4.1.7.3. 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;

10.2.4.1.7.4. 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.

10.2.4.1.8. 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.

10.2.4.1.9. 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.

10.2.4.1.10. 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.

10.2.4.1.11. 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.

10.2.4.1.12. 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;

10.2.4.1.13. 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.

10.2.4.1.14. 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.

10.2.4.1.15. 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.

10.2.4.1.16. 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

10.3. Requisitos de Nível de Serviço

10.3.1. O suporte técnico deverá estar disponível, no mínimo, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, mediante e-mail ou outro sistema de abertura que permita o registro com controle de histórico;

10.3.2. Disponibilidade para abertura de chamado: 24x7x365 (web, e-mail ou telefone);

10.3.3. Disponibilidade para início de atendimento na severidade máxima: até 2h dentro do horário do suporte técnico.

10.3.4. O tempo de solução será contabilizado entre a abertura do chamado e restabelecimento do sistema em sua totalidade.

10.3.5. O tempo de atendimento inicia-se com a primeira intervenção pelo representante da Contratada, local ou remotamente.

10.3.6. As multas por descumprimento de prazo serão aplicadas sobre os valores mensais do suporte técnico, sem prejuízo das demais sanções previstas neste Edital e Anexos.

10.3.7. Em caso de problema ou incidente de hardware ou de software, os seguintes prazos máximos deverão ser obedecidos para o início do atendimento e término da correção do problema:

eridade	**Descrição**	**SLA**
1 (severidade máxima)	Alteração de regras e políticas de segurança	Em até 1 hora

2 (severidade máxima)	Parada total da solução - mecanismos de contingência não funcionam; indisponibilidade total ou parcial das instâncias de um cluster no sítio; indisponibilidade total de um ou mais serviços das instâncias que compõem um sítio; degradação de serviços providos pelas instâncias que compõem o sítio; indisponibilidade ou degradação no mecanismo de balanceamento entre os sítios	Em até 1 hora
3 (severidade máxima)	Alteração de configurações	Em até 1 hora e 30 minutos
4 (severidade máxima)	Verificação de problemas de desempenho e/ou disponibilidade	Em até 3 horas
5	Verificação e filtragem de *logs*	Em até 1 hora
6	Esclarecimento de dúvidas/revisão de regras	Em até 24 hora
7	Aqueles para os quais houver solução de contorno cujo impacto não comprometa a operação dos serviços que utilizam a solução.	7 dias
8	Aqueles que não afetem o perfeito funcionamento da solução	7 dias

O descumprimento de quaisquer das obrigações assumidas importará na aplicação das seguintes penalidades:

Tempo decorrido entre o primeiro apontamento de indisponibilidade e a recuperação da disponibilidade do serviço	Multa
30 minutos	Sem aplicação de multa
60 minutos	0,5% do valor total mensal do respectivo item
120 minutos	1% do valor total mensal do respectivo item
180 minutos	1,5% do valor total mensal do respectivo item
240 minutos	2% do valor total mensal do respectivo item

10.4. Requisitos de capacitação

10.4.1. Conforme item 10.2.3.

10.5. Requisitos Suporte Técnico

10.5.1. Apoio a dúvidas de configurações, funcionamento, atualizações de versões;

10.5.2. Análises e soluções de alertas e problemas apresentados pela solução;

10.5.3. O atendimento será preferencialmente remoto. Caso haja necessidade de intervenção local, esta poderá ser executada. Nos dois casos, sempre com acompanhamento pela equipe técnica do STM, própria ou terceirizada.

10.5.4. Atendimento direto por técnicos do fabricante em português ou oferecer um tradutor;

10.5.5. Acesso web à base de conhecimento oficial;

10.5.6. Abertura ilimitada de chamados de suporte;

10.5.7. Possibilidade abertura de chamados via interface web, e-mail ou telefone.

10.6. Requisitos legais

Resolução CNJ N° 182/2013, dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ);

Resolução CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

LGPD – Lei Geral de Proteção de Dados (Lei no 13.709/2018) e Marco Civil da Internet Lei no 12.965/2014);

A Lei 8.666/1993, regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.

Plano de Contratações de 2023

10.7. Requisitos de manutenção

10.7.1. O suporte técnico deve iniciar logo após a assinatura do termo de aceite dos serviços de instalação e configuração e deverá ser realizado de forma contínua, e obrigatoriamente, pelo fabricante da ferramenta ou empresa prestadora de serviços devidamente credenciada;

10.7.2. Direito de atualização de software e pacotes de correção;

10.7.3. Direito de upgrade do produto para a última versão estável;

10.8. Requisitos Temporais

10.8.1. Os equipamentos e a instalação deverão ser entregues/disponibilizados no prazo de até 60 dias, após o recebimento da nota de empenho.

10.8.2. O item 3 deverá ser executado após após ou antes da instalação dos equipamentos, a critério do STM.

10.8.3.O item 4 deverá ser executado logo após assinatura do termo de aceite dos serviços de instalação e por período de 60 meses.

10.9. Requisitos Sociais, ambientais e culturais

10.9.1. Toda a documentação de software e base de conhecimento deverá estar disponível na internet, de forma a evitar impacto sobre recursos naturais decorrentes de produção de material de impressão, de pacotes e de desfazimento futuro

10.10 Requisitos de implantação

10.10.1. A instalação deverá ser nas dependências do STM.

10.10.2. A instalação deverá ser executada por técnico(s) qualificado(s) que possua(m), comprovadamente, vivência no ambiente de Virtualização VMWare.

10.11. Requisitos de garantia

10.11.1. O serviço de suporte envolverá todas as atividades necessárias para garantir a operação contínua do produto. Desta forma, farão parte do escopo das atividades de suporte:

a) Resolução de dúvidas e esclarecimentos relativos à utilização e configuração das funcionalidades;

b) Resolução de problemas que limitem ou impeçam o desenvolvimento e/ou execução de aplicações que façam uso efetivo das funcionalidades;

10.11.2. A CONTRATADA deverá disponibilizar canais de acesso 24 horas por dia, 7 dias por semana, através de número de telefone de discagem gratuita (0800) e/ou Internet, para abertura de chamados técnicos objetivando a resolução de problemas e dúvidas quanto ao funcionamento do produto. Todos os chamados, independente de sua criticidade, deverão ser abertos em um único número telefônico.

10.12. Requisitos de segurança da informação

10.12.1. O fornecedor deverá cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do STM.

10.12.2. Deverá, ainda, manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do objeto deste processo de contratação, respeitando todos os critérios de sigilo, segurança e inviolabilidade, aplicáveis aos dados, informações, regras de

negócio, documentos, entre outros.

10.12.3. As informações a serem tratadas de forma sigilosa, restrita e confidencial são aquelas que, por sua natureza, são consideradas como de interesse restrito ou confidencial, e não podem ser de conhecimento de terceiros, como por exemplo:

10.12.3.1. Dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, não podendo, sob qualquer pretexto serem divulgadas, reproduzidas ou utilizadas por terceiros sob pena de lei, independentemente da classificação de sigilo conferida pelo STM a tais documentos;

10.12.3.2. Resultados, parciais ou totais, sobre produtos gerados;

10.12.3.3. Programas de computador, seus códigos-fonte e códigos-objeto, bem como suas listagens e documentações;

10.12.3.4. Toda a informação relacionada a programas de computador existentes ou em fase de desenvolvimento no âmbito do STM e rotinas desenvolvidas por terceiros, incluindo fluxogramas, estatísticas, especificações, avaliações, resultado de testes, arquivo de dados, versões “beta” de quaisquer programas, dentre outros;

10.12.3.5. Documentos relativos à lista de usuários do STM e seus respectivos dados, armazenados sob qualquer forma;

10.12.3.6. Metodologias e ferramentas de serviços, desenvolvidas pelo STM;

10.12.3.7. Parte ou totalidade dos modelos de dados que subsidiam os sistemas de informações do STM, sejam eles executados interna ou externamente;

10.12.3.8. . Parte ou totalidade dos dados ou informações armazenadas nas bases de dados que subsidiam os sistemas de informações do STM, sejam elas residentes interna ou externamente;

10.12.3.9. Circulares e comunicações internas do STM;

10.12.3.10. Quaisquer processos ou documentos classificados como RESTRITO ou CONFIDENCIAL pelo STM.

10.13. DO CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS

10.13.1. As partes se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, nos termos da Lei Geral de Proteção de Dados - LGPD (Lei n. 13.709, de 14 de agosto de 2018).

10.13.2. É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

10.13.3. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contratual.

10.13.4. Os dados pessoais tornados públicos por este contrato deverão ser resguardados pelas partes, observados os princípios de proteção de dados previstos no art. 6º da Lei n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados).

10.13.5. A CONTRATADA fica obrigada a comunicar ao CONTRATANTE em até 24 (vinte e quatro) horas qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da Lei Geral de Proteção de Dados.

10.13.6. Durante toda a execução do objeto contratado, o tratamento de dados pessoais deverá se limitar ao mínimo necessário para a execução do objeto, sendo observados:

a) a compatibilidade com a finalidade especificada;

b) o interesse público; e

c) a regra de competência administrativa aplicável à situação concreta.

10.13.7. Os dados devem ser eliminados, quando não autorizada sua conservação, nos termos do art. 16 da LGPD, após o término de seu tratamento nas hipóteses previstas no art. 15 da referida lei.

10.13.8. A CONTRATADA deverá promover a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE em caso de desligamento de funcionário

das atividades inerentes à execução do presente Contrato.

10.13.9. A CONTRATADA não poderá disponibilizar ou transmitir a terceiros, sem prévia autorização por escrito, informação, dados pessoais ou base de dados a que tenha acesso em razão do cumprimento do objeto contratual.

10.13.10. Encerrada a vigência do contrato ou após a satisfação da finalidade pretendida, a CONTRATADA interromperá o tratamento dos dados pessoais disponibilizados pelo CONTRATANTE e, em no máximo trinta dias, sob instruções e na medida do determinado por este, eliminará completamente os Dados Pessoais e todas as cópias porventura existentes (seja em formato digital ou físico), salvo quando a CONTRATADA tenha que manter os dados para cumprimento de obrigação legal.

10.13.11. A CONTRATADA ficará obrigada a assumir total responsabilidade pelos danos patrimoniais, morais, individuais ou coletivos que venham a ser causados em razão do descumprimento de suas obrigações legais no processo de tratamento dos dados compartilhados pelo CONTRATANTE.

10.13.12. Eventuais responsabilidades serão apuradas de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

11. CERTIFICAÇÕES E COMPATIBILIDADES

Os serviços deverão ser executados por técnico(s) qualificado(s) que possua(m), comprovadamente, vivência no equipamento instalado.

12. ENTREGA DA SOLUÇÃO

12.1. Prazo de entrega/disponibilização dos produtos: no máximo 60 (sessenta) dias corridos a partir do recebimento da nota de empenho.

12.2. O descumprimento ao prazo citado sujeitará a EMPRESA CONTRATADA a penalidade de multas previstas no edital.

13. LOCAL DE INSTALAÇÃO

13.1. A instalação da solução do grupo 1 deverá ser feita na sede do Superior Tribunal Militar - Setor de Autarquias Sul, Praça dos Tribunais Superiores - Cep.: 70.098-900 - Brasília - DF

14. OBRIGAÇÕES DA CONTRATADA

14.1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade especificadas neste Termo de Referência e em sua proposta.

14.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

14.3. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor.

14.4. Apresentar os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso.

14.5. Apresentar à CONTRATANTE, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço.

14.6. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE.

14.7. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração.

14.8. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a CONTRATADA relatar à CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função.

14.9. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.

14.10. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

14.11. Manter durante toda a execução do objeto e vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

14.12. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

14.13. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

14.14. Assegurar à Contratante:

14.14.1. O direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo à CONTRATANTE distribuir, alterar e utilizar estes sem limitações; e

14.14.2. Os direitos autorais da solução, do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua utilização sem que exista autorização expressa da CONTRATANTE, sob pena de multa, sem prejuízo das sanções civis e penais cabíveis.

14.15. Deter instalações, aparelhamento e pessoal técnico adequado, disponíveis para a realização do objeto da licitação.

15. CONTRATANTE

15.1. Designar gestor que efetuará sua representação perante a CONTRATADA para determinação, avaliação, acompanhamento e aprovação dos serviços por ela realizados;

15.2. Prestar os esclarecimentos que venham a ser solicitados pela CONTRATADA, no que diz respeito ao contrato;

15.3. Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal nº 8.666/1993 e suas alterações posteriores.

15.4. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

15.5. Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.

15.6. Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste Termo.

15.7. Aplicar as penalidades previstas em lei e neste instrumento.

16. SIGILO DAS INFORMAÇÕES

16.1. A CONTRATADA obriga-se, durante o curso do Contrato e após o seu término, ao mais completo e absoluto sigilo com relação a toda informação de qualquer natureza referente às atividades do CONTRATANTE, das quais venha a ter conhecimento ou venha a ter acesso por força do cumprimento do presente Contrato, não podendo sob qualquer pretexto, utilizá-las para si, invocar, revelar, reproduzir ou delas dar conhecimento a terceiros, responsabilizando-se em caso de descumprimento da obrigação assumida por eventuais perdas e danos e sujeitando-se às cominações legais, nos termos da Lei 4.595 de 31.12.1964 e demais leis correlatas;

16.2. “Informações Confidenciais" significam os dados ou informações confidenciais desenvolvidas ou adquiridas pelo CONTRATANTE ou pela Licitante vencedora e cuja divulgação ou utilização não autorizada, por qualquer das partes, poderá ser prejudicial a um ou a outro;

16.3. O CONTRATANTE e a Licitante vencedora tratarão sigilosamente todas as informações confidenciais, produtos e materiais que as contenham, não podendo ser copiados ou reproduzidos, publicados, divulgados ou de outra forma colocados à disposição, direta ou indiretamente, de qualquer pessoa, a não ser empregados e agentes do CONTRATANTE e/ou da Licitante vencedora que deles necessitem para desempenhar as suas funções no CONTRATANTE, sem que para tanto seja devido o consentimento prévio do CONTRATANTE ou comunicado da empresa vencedora;

16.4. As partes se obrigam a instruir sua equipe e prepostos a respeito das presentes disposições, as quais deverão ser observadas mesmo após o término ou cancelamento do futuro CONTRATO.

17. DIREITOS DE PROPRIEDADE, MARCAS, PATENTES E DIREITOS AUTORAIS

17.1. Quaisquer reproduções ou cópias de produtos e/ou bens e direitos cujos direitos de propriedade, marcas, patentes ou direitos autorais estiverem sob a responsabilidade da LICITANTE vencedora resultantes dos Serviços, incluindo documentação a eles correlata, em qualquer idioma, que forem desenvolvidos especificamente pela Licitante vencedora (para o CLIENTE) sob os dispositivos do futuro CONTRATO são de propriedade exclusiva do CONTRATANTE e deverão: (I) ser claramente designados como confidenciais, (II) incluir todas as marcas e indicações que façam referência ao proprietário, conforme apropriado, e (III) ter o mesmo grau de confidencialidade, proteção e legitimidade do original.

18. DA FISCALIZAÇÃO E ACOMPANHAMENTO

18.1. O acompanhamento e a fiscalização do contrato caberão à Equipe de Gestão do Contrato, que será instituída pelo Diretor-Geral, após a assinatura das partes;

18.2. No momento da assinatura do Contrato, a Contratada indicará um preposto para representá-la, sendo este responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao Contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual;

18.3. Assinado o contrato, o Diretor-Geral do Contratante instituirá a Equipe de Gestão da Contratação, composta por:

18.3.1. Gestor do Contrato: servidor com atribuições gerenciais, técnicas ou operacionais, relacionadas ao processo de gestão do contrato, para coordenar, supervisionar e controlar a execução do contrato, a fim de garantir o atendimento dos objetivos do Contratante;

18.3.2. Fiscal Demandante do Contrato: servidor representante da Diretoria de Tecnologia da Informação, competente para fiscalizar o contrato quanto aos aspectos funcionais da solução;

18.3.3. Fiscal Técnico do Contrato: servidor representante da Área da Diretoria de Tecnologia da Informação, competente para fiscalizar o contrato quanto aos aspectos técnicos da solução;

18.3.4. Fiscal Administrativo do Contrato, servidor representante da Área Administrativa, competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

18.4. A existência e a atuação da fiscalização pelo Contratante em nada restringe a responsabilidade, única, integral e exclusiva da Contratada, no que concerne à execução do contrato.

19. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

19.1. A Equipe de Planejamento desta contratação é composta pelos servidores Wilson Marques de Souza Filho (Integrante Demandante), Márcio Coelho Marques (Integrante Técnico) e Luis Gustavo Costa Reis (Integrante Administrativo).

19.2. A indicação do Integrante Administrativo consta do Documento de Oficialização da Demanda – DOD, de acordo com o inc. III, do § 5º, do art. 12, da Resolução nº 182, de 17 de outubro de 2013, do Conselho Nacional de Justiça.

19.3. A Equipe de Planejamento da Contratação foi instituída pelo Senhor Diretor-Geral, em conformidade com o inc. IV, do § 7º, do art. 12, da mesma Resolução.

20. EQUIPE DE APOIO À CONTRATAÇÃO

A Equipe de Apoio à Contratação é composta pelos integrantes da Equipe de Planejamento da Contratação e tem como finalidade subsidiar a Área de Licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes (redação dada pelo inc. XI, do art. 2º, da Resolução nº 182/13, do CNJ).

21. VIGÊNCIA DO CONTRATO

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

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

21.3. A vigência do contrato referente ao item 4 será de 60 meses, a contar da assinatura do termo de aceite dos serviços de instalação.

22. PAGAMENTO

22.1. O pagamento referente aos itens 1,2 e 3 será efetuado em parcela única, após a entrega do objeto.

22.2. O pagamento referente ao Item 4 deverá ser efetuado em parcelas mensais,

22.3. Para efeitos de pagamento, a CONTRATADA deverá apresentar documento de cobrança constando, de forma discriminada a efetiva realização do objeto adquirido, informando o nome e numero do banco, a agência e o número da conta corrente em que o crédito deverá ser efetuado.

22.4. Deverá apresentar juntamente com o documento de cobrança a comprovação de que cumpriu as seguintes exigências, cumulativamente:

22.4.1. Certidão de regularidade com a Seguridade Social;

22.4.2. Certidão de regularidade com o FGTS;

22.4.3. Certidão de regularidade com a Fazenda Federal;

22.4.4. Certidão Negativa de Débitos Trabalhistas;

22.4.5. Certidão de regularidade com a Fazenda Estadual e Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da Lei.

22.5. Os documentos de cobrança deverão ser enviados via peticionamento eletrônico.

Caso o objeto contratado seja faturado em desacordo com as disposições previstas no Edital e neste Termo de Referência ou sem a observância das formalidades legais pertinentes, a CONTRATADA deverá emitir e apresentar novo documento de cobrança, não configurando atraso no pagamento.

22.6. Após o atesto do documento de cobrança, que deverá ocorrer no prazo de até 05 (cinco) dias úteis contado do seu recebimento, o responsável deverá encaminhá-lo para pagamento.

22.7. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido de Alguma forma para o fato, a atualização financeira devida, entre a data que deveria ser efetuado o pagamento e a data correspondente ao efetivo pagamento, será calculada da seguinte forma, devendo a atualização prevista nesta condição ser incluída em nota fiscal a ser apresentada posteriormente:

AF = I x N x VP , onde:

AF = atualização financeira devida;

I = 0,0001644 (índice de atualização dia);

N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = valor do pagamento devido.

23. DO REAJUSTE DE PREÇOS

23.1. O valor dos itens 1, 2 e 3, objeto desta licitação, são fixos e irreajustáveis.

23.2. Para o item 03, poderá haver reajuste anual de preços para as parcelas do contrato, de acordo com o Índice de Custo da Tecnologia da Informação (ICTI), do Instituto de Pesquisa Econômica Aplicada (IPEA), ou outro índice que venha a ser adotado pelo Governo Federal, em substituição àquele, observado o interregno mínimo de

um ano a partir da data da proposta:

22.2.1. o pedido de reajuste de preços deverá ocorrer antes da assinatura do termo de prorrogação contratual, sob pena de preclusão.

22.3. Para efeito de cálculo dos reajustes será utilizada a seguinte fórmula:

$$R = V \frac{I - IO}{IO}$$, onde:

R = valor do reajustamento procurado;

V = valor contratual do serviço;

I = valor do índice relativo ao mês do reajuste, conforme definido no contrato;

IO = valor do índice inicial, correspondente ao mês da apresentação da proposta.

22.4. Por ocasião do pedido de reajuste, caberá à Contratada apresentar planilha dos cálculos, de acordo com fórmula do item 22.2.

22.5. Caberá à Contratada, por ocasião do reajustamento de preços, apresentar faturas distintas, sendo uma correspondente aos preços iniciais contratados e outra, suplementar, relativa ao valor do reajustamento devido e pactuado pelas partes.

22.6. Ocorrendo o primeiro reajuste, os subsequentes só poderão ocorrer obedecendo ao prazo mínimo de um ano, a contar do início dos efeitos do último reajuste.

22.7. O reajuste de que trata o Item 22.1 poderá sofrer alteração posterior, total ou parcial, decorrente da adoção, pelo Governo Federal, de medidas ou normas financeiras com força de lei.

24. RESCISÃO CONTRATUAL

24.1. A inexecução total ou parcial do contrato enseja a sua rescisão, conforme disposto nos arts. 77 a 80 da Lei no 8.666/93:

24.1.1. Os casos de rescisão contratual deverão ser formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

24.2. A rescisão do contrato poderá ser:

24.2.1. Determinada por ato unilateral e escrito do Contratante, nos casos enumerados nos incisos I a XII, XVII e XVIII, do art. 78 da Lei nº 8.666/93;

24.2.2. Amigável, por acordo entre as partes, desde que haja conveniência para o Contratante;

24.2.3. Judicial, nos termos da legislação vigente sobre a matéria.

24.3. A rescisão administrativa ou amigável será precedida de autorização escrita e fundamentada da autoridade competente.

25. DESPESA ORÇAMENTÁRIA

25.1. A despesa ocorrerá à conta de dotação consignada à Justiça Militar da União pela Lei Orçamentária para o exercício de 2023, por meio dos seguintes Encargos do Plano de Ação (Código e Identificação) e emissão de respectivas Notas de Empenho:

25.1.1. As despesas decorrentes da presente contratação serão provenientes do Programa de Trabalho: SEG0; Elemento de Despesa 3.3.90.40

26. ACRÉSCIMO OU SUPRESSÃO DO OBJETO

26.1. A critério da Administração, o objeto desta licitação poderá ser acrescido ou suprimido em até 25% do valor inicial contratado atualizado, observado o disposto no art. 65, §§ 1º e 2º, da Lei nº 8.666/93.

26.2. O acréscimo ou supressão contratual não poderá exceder os limites estabelecidos no § 1º do art. 65 da Lei nº 8.666/93, salvo a supressão decorrente de acordo celebrado entre as partes.

27. CONSIDERAÇÕES GERAIS

27.1. A equipe técnica envolvida na prestação dos serviços deverá possuir conhecimento e experiência conforme os requisitos técnicos para a prestação dos serviços descritos neste Termo de Referência;

27.2. A CONTRATADA, às suas expensas, deverá disponibilizar um profissional destacado para a gestão do relacionamento com a CONTRATANTE, o qual, além de possuir conhecimentos e capacidade profissionais necessários, deverá ter competência para resolver imediatamente todo e qualquer assunto relacionado com os serviços contratados;

27.3. A ausência ou omissão da fiscalização do CONTRATANTE não eximirá a CONTRATADA das responsabilidades oriundas deste contrato;

27.4. Todos os softwares e recursos computacionais utilizados pela CONTRATADA, necessários para o atendimento do objeto do contrato, deverão ser devidamente legalizados, em conformidade com as leis de Software (nº 9.609/98) e do Direito Autoral (nº 9.610/98);

27.5. Caso haja a necessidade de alocar equipamentos de informática nas dependências do CONTRATANTE, de propriedade da CONTRATADA, como computadores, switches, hubs, roteadores e impressoras, estes, obrigatoriamente, antes de conectar-se com a rede corporativa, deverão estar de acordo com a Política de Segurança da CONTRATANTE.

27.6. Caso haja necessidade de acessos remotos, por parte dos funcionários da CONTRATADA, o CONTRATANTE deverá ser informado, por escrito, da necessidade de utilização do referido meio e a CONTRATADA deverá ratificar que está de acordo com a Política de Segurança da Informação e o Termo de Confidencialidade, respectivamente;

28. SANÇÕES ADMINISTRATIVAS

28.1. Com fundamento no art. 7º da Lei n. 10.520/2002 e nos artigos 86 e 87 da Lei n. 8.666/1993, a CONTRATADA ficará sujeita, assegurada prévia e ampla defesa, às seguintes penalidades:

a) advertência;

b) multa nas condições e percentuais estabelecidos no Termo de Referência;

c) suspensão temporária de participação em licitação e impedimento de contratar com o CNJ, por prazo não superior a 2 (dois) anos;

d) impedimento de licitar e contratar com a União e descredenciamento do SICAF, pelo prazo de até 5 (cinco) anos;

e) declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada com base na alínea “c” dessa cláusula.

28.2. O valor da multa, aplicada após o regular processo administrativo, será descontado de pagamentos eventualmente devidos pelo CONTRATANTE à CONTRATADA, da garantia contratual ou cobrado judicialmente.

28.3. As sanções previstas nas alíneas "a", "c" e “e” do caput desta cláusula poderão ser aplicadas, cumulativamente ou não, à pena de multa.

28.4. A penalidade prevista na alínea "d" desta cláusula também poderá ser aplicada à CONTRATADA, caso tenha sofrido condenação definitiva por fraudar recolhimento de tributos, praticar ato ilícito visando frustrar os objetivos da licitação ou demonstrar não possuir idoneidade para contratar com a Administração.

28.5. Excepcionalmente, desde que devidamente justificado no processo administrativo, o CONTRATANTE poderá efetuar a retenção do valor presumido da multa, e, concomitantemente, instaurar regular processo administrativo oportunizando à CONTRATADA o exercício do contraditório e da ampla defesa.

28.6. As penalidades serão obrigatoriamente registradas no SICAF, e sua aplicação deverá ser precedida da concessão da oportunidade de ampla defesa para CONTRATADA, na forma da lei.

28.7. Os instrumentos de requerimentos, de defesas prévias e de recursos eventualmente interpostos pela CONTRATADA deverão ser instruídos com os documentos hábeis à prova das alegações neles contidas.

28.7.1. Referidos documentos probatórios deverão ser apresentados em suas versões originais e/ou em versões autenticadas, por cartórios extrajudiciais ou por servidores da Administração Pública, sob pena de, a critério exclusivo do

CONTRATANTE, não serem avaliados.

29. FUNDAMENTO LEGAL

A elaboração deste Termo de Referência fundamenta-se no disposto na Lei nº 10.520, de 17 de julho de 2002, nos Decretos nº 10.024, de 20 de setembro de 2019, na Resolução nº 182, de 17 de outubro de 2013, do Conselho Nacional de Justiça, e, subsidiariamente, na Lei nº 8.666, de 21 de junho de 1993.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		
Em cumprimento ao exposto no § 1º do art. 13 da Resolução nº 182, de 17 de outubro de 2013, do Conselho Nacional de Justiça, a Equipe de Planejamento da Contratação submete os Estudos Preliminares e o Termo de Referência à aprovação do Diretor de Tecnologia da Informação, titular da Área Demandante.		
INTEGRANTE TÉCNICO	**INTEGRANTE DEMANDANTE**	**INTEGRANTE ADMINISTRATIVO**
Márcio Coelho Marques	**Wilson Marques de Souza Filho**	**Luis Gustavo Costa Reis**
VALIDAÇÃO DO TERMO DE REFERÊNCIA		
Autoridade da Área Demandante - Ianne Carvalho Barros - Diretor da DITIN		

Documento assinado eletronicamente por **WILSON MARQUES DE SOUZA FILHO**, **COORDENADOR DE TECNOLOGIA**, em 16/08/2023, às 16:14 (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 16/08/2023, às 16:37 (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 16/08/2023, às 17:26 (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 16/08/2023, às 18:02 (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 **3336608** e o código CRC **20D43392**.

Setor de Autarquias Sul, Praça dos Tribunais Superiores - Bairro Asa Sul - CEP 70098-900 - Brasília - DF - http://www.stm.jus.br/