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

ESTUDO TÉCNICO PRELIMINAR - TIC

ESTUDO TÉCNICO PRELIMINAR - TIC

CONFORME A RESOLUÇÃO CNJ Nº 468/2022 E O

GUIA DE CONTRATAÇÕES DE SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (STIC) - VERSÃO 4.0

Histórico de Revisões

Data	Versão	Descrição	Autor
27/3/2025	1.0	Finalização da primeira versão do documento	Equipe de Planejamento
06/06/2025	2.0	Revisão do documento	Equipe de Planejamento
16/07/2025	3.0	Inclusão das propostas	Equipe de Planejamento
29/08/2025	4.0	Revisão	Equipe de Planejamento

ESTUDO TÉCNICO PRELIMINAR

1. CAPÍTULO 1: ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. Contextualização

1.1.1. Problema a ser resolvido sob a perspectiva do interesse público:

A necessidade dessa contratação de Serviços Gerenciado de Segurança da Informação, surge do contexto de evolução tecnológica e da globalização, que impõem desafios significativos e favorecem o surgimento de crimes virtuais complexos. Para um órgão governamental como a Justiça Militar da União (JMU), a modernização dos serviços e a proteção contra ameaças digitais são cruciais para otimizar a prestação de serviços e o atendimento ao público.

A atualização contínua das ferramentas de segurança da informação é fundamental para antecipar essas ameaças e proteger a JMU de prejuízos incalculáveis que poderiam ser causados por ataques cibernéticos. Isso é indispensável para garantir a continuidade e estabilidade dos serviços, minimizando interrupções e indisponibilidade dos sistemas.

Além disso, a complexidade das soluções de segurança requer suporte técnico especializado, fornecido por empresas certificadas e com experiência em ambientes corporativos críticos. A experiência demonstra a importância desse suporte para a resolução de problemas, gerenciamento de novas versões de software, instalação, configuração e implementação de regras de segurança e tratamento de incidentes.

Essa demanda está alinhada aos esforços do Superior Tribunal Militar (STM) para aprimorar seu parque tecnológico e reforçar a segurança, bem como às diretrizes e normativos superiores. Especificamente, atende à necessidade de prover a segurança cibernética e proteção de dados, conforme as recomendações da Política de Segurança Cibernética da JMU e da Resolução CNJ nº 396/2021. A contratação também visa atender aos requisitos mínimos de segurança para investigação de ilícitos cibernéticos, conforme a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética no âmbito do Poder Judiciário. No PDTIC 2025-2026, "Ataques cibernéticos" são identificados como uma ameaça externa, e "Aprimorar Segurança da Informação e a Gestão de Dados" é um objetivo estratégico (OE6), justificado pela importância estratégica de proteger informações sensíveis e valiosas da JMU. A ENTIC-JUD (Resolução CNJ nº 370/2021) também destaca o "Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados" como um macrodesafio e inclui "Aprimorar a Segurança da Informação e a Gestão de Dados" (Objetivo 7).

Portanto, a contratação se justifica pela necessidade premente de fortalecer a postura de segurança cibernética da JMU diante de ameaças crescentes, garantir a continuidade dos serviços públicos essenciais e cumprir com as determinações estratégicas e regulatórias no âmbito do Poder Judiciário, protegendo dados e sistemas em benefício do interesse público.

1.2. Identificação da demanda no Plano de Contratações de STIC -

No PCA 2025 Tecnologia, a demanda está classificada sob a descrição "Serviços De Gerenciamento Em Tecnologia Da Informação E Comunicação (TIC)

1.2.1. Alinhamento da Solução

A contratação proposta está em total alinhamento com os principais instrumentos de planejamento estratégico e normativas no âmbito do Poder Judiciário e da Justiça Militar da União:

Planejamento Estratégico da JMU (PEJMU 2021-2026 - Resolução STM nº 289/2020): A demanda atende diretamente a objetivos estratégicos cruciais, conforme explicitado no DOD e detalhado no PEJMU:

Objetivo 4: Fortalecer a governança e a segurança de dados e informações. Este objetivo foca no aprimoramento da gestão de políticas, processos, pessoas e tecnologia relacionados a dados e informações, buscando a proteção de dados pessoais e institucionais. A contratação de serviços gerenciados de segurança cibernética com NGFW, SD-WAN e XDR é fundamental para a consecução deste objetivo.

Objetivo 11: Otimizar a infraestrutura e as soluções de tecnologia da informação e comunicação (TIC) para atender as necessidades da JMU. Este objetivo visa compatibilizar a infraestrutura e as soluções de TIC com os desafios da JMU, incluindo hardware, software, gestão de rede e telecomunicações. A modernização da proteção de perímetro com NGFW e SD-WAN é uma ação direta para otimizar a infraestrutura de rede.

Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC 2025-2026 - Resolução STM nº 349/2024): O PDTIC da JMU foi elaborado em consonância com o Planejamento Estratégico da JMU e a ENTIC-JUD.

Ameaças externas identificadas no diagnóstico do PDTIC incluem "Ataques cibernéticos".

A contratação se alinha ao Objetivo Estratégico OE6: Aprimorar a Segurança da Informação e a Gestão de Dados. Este objetivo estratégico justifica a importância de proteger informações sensíveis e valiosas.

O PDTIC lista ações no tema "Segurança Cibernética", mencionando a implantação de soluções como UTM (firewall), XDR (2024/2025), e NOC/SOC/SIEM (2025/2026). A contratação proposta, incluindo NGFW (tipo de firewall), SD-WAN, XDR e gerenciamento centralizado, abrange e suporta diretamente essas ações planejadas no PDTIC.

Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD - Resolução CNJ nº 370/2021): A ENTIC-JUD institui diretrizes para a TIC no Poder Judiciário, alinhadas aos macrodesafios, especialmente o "Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados".

A contratação contribui para o alcance do Objetivo Estratégico 7: Aprimorar a Segurança da Informação e a Gestão de Dados da ENTIC-JUD.

As diretrizes da ENTIC-JUD preveem temas como "Riscos, Segurança da Informação e Proteção de Dados" e exigem a elaboração de Plano de Gestão de Riscos de TIC e a aplicação de práticas e processos de segurança da informação e proteção de dados. A solução de segurança gerenciada aborda esses requisitos.

Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ - Resolução CNJ nº 396/2021): A ENSEC-PJ é explicitamente mencionada como base para a justificativa da demanda no PCA. Esta resolução institui a Estratégia Nacional de Segurança Cibernética no âmbito do Poder Judiciário. A contratação de serviços e equipamentos para proteção de perímetro e detecção e resposta a ameaças é uma implementação direta das diretrizes e requisitos mínimos de segurança para investigação de ilícitos cibernéticos contidos nesta Resolução.

Política de Segurança Cibernética da JMU (Resolução STM N° 350/2024) e Política de Segurança da Informação da JMU (Resolução STM N° 351/2024): Mencionadas como recomendações no PCA e listadas como referências estratégicas do PDTIC, estas políticas internas estabelecem as diretrizes e controles para a segurança cibernética e da informação na JMU. A contratação dos serviços e equipamentos de segurança de perímetro visa implementar e reforçar a aplicação dessas políticas.

Em resumo, a contratação está devidamente planejada no PCA e alinhada a múltiplos níveis de planejamento estratégico (PEJMU, PDTIC) e normativos (ENTIC-JUD, ENSEC-PJ, Políticas de Segurança da JMU), todos convergindo para a necessidade imperativa de fortalecer a segurança cibernética e otimizar a infraestrutura de TIC da JMU, em benefício do interesse público e da continuidade dos serviços essenciais.

1.3. Caracterização da demanda

1.3.1. Definição e Especificação das Necessidades

A necessidade primordial que impulsiona esta contratação é a proteção dos ativos de informação e a garantia da continuidade dos serviços jurisdicionais da Justiça Militar da União (JMU)1111. Em um cenário de crescente sofisticação dos ataques cibernéticos, a infraestrutura atual de segurança de perímetro, embora funcional, necessita de uma modernização tecnológica e de um novo modelo de gestão para fazer frente às ameaças complexas e persistentes

A necessidade de quatro tipos distintos de equipamentos para proteção de perímetro do tipo NGFW com SD-WAN (Tipo I, II, III, e IV) decorre da diversidade de requisitos de desempenho, capacidade e conectividade demandados pelos diferentes pontos da rede da Contratante, a Justiça Militar da União (JMU).

1. Tipo I (Concentrador): São necessárias 2 unidades que atuarão como concentradores.

2. Tipo II (Unidade Remota): É necessária 1 unidade. Conforme sua especificação, esta unidade será utilizada na garagem do STM, onde está localizado o backup, exigindo interfaces de rede de 10Gbps ou superior.

3. Tipo III (Unidades Remotas): São necessárias 3 unidades. Estas serão instaladas nas Auditorias do Rio de Janeiro, São Paulo e Brasília. Possuem requisitos de desempenho e capacidade inferiores ao Tipo II, mas ainda significativos.

4. Tipo IV (Unidades Remotas): São necessárias 12 unidades. Estas serão instaladas nas demais Auditorias. Representam o equipamento com os requisitos de desempenho e capacidade mínimos.

A divisão em tipos otimiza o custo da solução ao dimensionar os equipamentos conforme a demanda real de cada localidade, ao invés de usar um modelo único que seria superdimensionado para a maioria das unidades ou subdimensionado para o concentrador e o site de backup.

As necessidades tecnológicas e de negócio que motivam esta contratação são:

· **Proteção Abrangente de Perímetro:** Implementar uma barreira de segurança avançada na fronteira da rede para inspecionar, controlar e proteger o tráfego de entrada e saída contra uma vasta gama de ameaças, incluindo malware, invasões e ataques de dia zero.

· **Otimização da Conectividade e Desempenho de Rede:** Utilizar a tecnologia SD-WAN para gerenciar múltiplos links de rede de forma inteligente, garantindo a qualidade de serviço (QoS) para aplicações críticas, a resiliência da conexão e a otimização do uso da largura de banda.

· **Gerenciamento Centralizado e Eficiente:** A necessidade de uma solução que permita o gerenciamento unificado de todas as funcionalidades de segurança e SD-WAN, simplificando a administração, monitoramento e geração de relatórios.

· **Disponibilidade e Continuidade:** Garantir que os serviços de segurança e conectividade permaneçam operacionais, mesmo diante de falhas ou incidentes, com mecanismos de redundância e alta disponibilidade.

· **Conformidade e Governança:** Atender às políticas de segurança da informação e proteção de dados da instituição, bem como às normativas do Conselho Nacional de Justiça (CNJ), especialmente a Resolução CNJ nº 396/2021 (Estratégia Nacional de Segurança Cibernética do Poder Judiciário).

· **Suporte Especializado e Dedicado:** Contar com profissionais qualificados e dedicados para a instalação, configuração, operação assistida, resolução de problemas e ajuste de políticas, liberando a equipe interna de TI para outras atividades estratégicas.

1.3.2. Definição e Especificação de Requisitos

Os requisitos técnicos e funcionais detalhados a seguir foram formulados para atender integralmente às necessidades descritas. Eles representam o conjunto de capacidades, desempenhos e funcionalidades que a solução contratada deverá obrigatoriamente possuir para ser considerada tecnicamente viável e aderente aos objetivos estratégicos do STM.

1.3.3. Requisitos Funcionais

Os requisitos a seguir são transcritos e justificados com base na estrutura do documento de Especificação Técnica Detalhada.

1.3.3.1. Requisitos de arquitetura tecnológica (Configuração):

1.3.3.1.1. Características Gerais do Serviço Gerenciado

Esta seção define o escopo e as condições gerais da prestação de serviço, assegurando transparência, segurança jurídica e o alinhamento com as necessidades de gestão do STM.

a) Requisito: As licenças (subscrição) dos softwares que compõem os itens 1, 2, 3 e 4 do grupo 1 devem ser emitidas no nome da contratante.

Justificativa: Garante a posse legal e o direito de uso dos ativos de software pelo STM. Essa condição é fundamental para a gestão de ativos de TIC, conformidade em auditorias e, crucialmente, para evitar a dependência excessiva (vendor lock-in), assegurando a continuidade operacional caso haja uma futura troca do prestador de serviço.

b) Requisito: Sobre os itens 1, 2, 3 e 4 do grupo 1, especificar os custos envolvidos com licenças de softwares e outros custos (pessoas).

Justificativa: Promove a transparência na composição de preços da proposta. A segregação de custos permite ao STM avaliar a economicidade de cada componente do serviço (o custo do licenciamento vs. o custo do serviço gerenciado/pessoal), facilitando a análise comparativa com o mercado e o planejamento orçamentário para futuras renovações ou expansões.

c) Requisito: Caso seja necessário substituir licenças equivalentes durante a vigência do contrato, isso deverá ocorrer sem qualquer ônus para a contratante8.

Justificativa: Mitiga o risco tecnológico e financeiro associado ao ciclo de vida dos produtos. Fabricantes podem descontinuar linhas de produtos ou modelos de licenciamento. Esta cláusula protege o investimento do STM, garantindo que o nível de serviço e as funcionalidades contratadas serão mantidos com tecnologia equivalente ou superior sem custos adicionais imprevistos.

d) Requisito: Os equipamentos de proteção de perímetro com SD-WAN que compõem o serviço devem ser novos e sem uso anterior, em linha de produção e fornecidos em sua versão mais atualizada.

Justificativa: Assegura que o STM receberá uma solução tecnológica de ponta, com o máximo de vida útil, garantia integral do fabricante e as mais recentes correções de segurança e funcionalidades. Isso evita o recebimento de equipamentos recondicionados ou próximos do fim de vida (End-of-Life), que representam maior risco de falhas e menor janela de suporte.

e) Requisito: Fornecimento de monitoração e gerenciamento através de SOC/NOC para todos os equipamentos, com a CONTRATADA sendo responsável por implementar e gerenciar as políticas de segurança definidas pelo cliente10.

Justificativa: Este é o cerne do modelo de "Serviço Gerenciado". Ele transfere a responsabilidade da operação, monitoramento 24x7 e resposta inicial a incidentes para a contratada, que possui um Centro de Operações de Segurança/Rede (SOC/NOC). Isso libera a equipe interna da DITIN de tarefas operacionais intensivas, permitindo foco em ações estratégicas, ao mesmo tempo que garante vigilância contínua e especializada do ambiente.

f) Requisito: Fornecimento de um profissional sênior, dedicado de forma exclusiva e contínua, para gerenciamento e administração de todos os serviços e equipamentos.

Justificativa: Dada a criticidade e complexidade da solução, um ponto focal de alta especialização é indispensável. A dedicação exclusiva garante que o profissional terá um conhecimento profundo e contextualizado do ambiente do STM, resultando em maior agilidade no suporte avançado (Nível 2 e 3), proatividade na otimização de políticas e eficácia na resolução de problemas complexos, servindo como uma extensão qualificada da equipe da COTEC.

1.3.3.2. Especificações Técnicas Mínimas dos Equipamentos

1.3.3.2.1. Equipamento Tipo I (Concentrador - Sede/Data Center)

a) Requisito: Desempenho de Next Generation Firewall de 19 Gbps, 8 Gbps com todas as funcionalidades de segurança ativas, e 3.6 Gbps para tráfego com inspeção SSL/TLS.

Justificativa: Estas métricas de desempenho são críticas para o Data Center, que concentra todo o tráfego da JMU. O alto desempenho garante a inspeção profunda de todo o tráfego, inclusive o criptografado (onde ameaças se ocultam), sem criar gargalos que afetem a performance dos sistemas judiciais e administrativos.

b) Requisito: Suporte a 240.000 novas conexões/segundo e 3.000.000 de conexões simultâneas.

Justificativa: A alta taxa de novas conexões é vital para suportar picos de acesso. O alto número de conexões simultâneas é necessário para manter a estabilidade de todas as sessões ativas dos usuários, sistemas e serviços.

c) Requisito: Fonte de alimentação redundante.

Justificativa: Requisito básico de alta disponibilidade. Evita que a falha de um componente de energia cause a interrupção completa do acesso à rede, garantindo a continuidade dos serviços.

d) Requisito: Alta densidade de interfaces de rede (8x 10/100/1000 Base-T, 8x 10Gbps SFP+, 4x 25Gbps SFP28).

Justificativa: Necessário para a interconexão com a rede de alta velocidade do Data Center do STM, incluindo switches de core, servidores e outros equipamentos, garantindo uma arquitetura moderna e escalável.

e) Requisito: Possuir interface dedicada e física para gerenciamento do equipamento fora de banda (Out-of-Band Management). Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Não sendo permitido qualquer tipo de configuração via software para esta função.

Justificativa : Este requisito é um pilar fundamental para a resiliência, a recuperabilidade e a gestão segura da infraestrutura crítica de segurança do STM. A exigência de uma interface de gerenciamento física e verdadeiramente fora de banda vai além de uma simples conveniência administrativa; ela é uma salvaguarda essencial contra cenários de falha que poderiam comprometer toda a operação da Justiça Militar da União.

1. Garantia de Continuidade Operacional e Resiliência em Cenários de Falha Crítica: O firewall de perímetro é um dos ativos mais críticos da rede. Uma falha neste equipamento resulta na interrupção total da comunicação, paralisando serviços essenciais como o e-Proc/JMU. A interface fora de banda, por ser um canal físico e eletronicamente independente, funciona como uma "UTI" para o equipamento, provendo um caminho alternativo e direto para a equipe de TI realizar ações de emergência, mesmo que o "cérebro" principal do equipamento esteja incapacitado.

2. Redução Drástica do Tempo Médio de Reparo (MTTR): Sem uma interface OOB, a única solução para uma falha crítica é o deslocamento físico de um técnico ao Data Center, processo que pode levar horas. Com a gerência OOB, o Tempo Médio de Reparo (MTTR) é reduzido para minutos, pois a equipe da DITIN pode acessar a console de emergência de forma remota e imediata (24x7) para iniciar a recuperação.

3. Segurança e Confiabilidade da Gestão do Dispositivo: A exigência de ser física e dedicada garante que o canal de recuperação seja verdadeiramente independente do sistema operacional principal, que pode estar travado. Adicionalmente, este canal é inerentemente mais seguro, pois fica isolado em uma rede de gerenciamento restrita, protegido de ameaças da rede principal.

f) Requisito : Arquitetura modular de interfaces de rede.

Justificativa: Garante a proteção do investimento e a flexibilidade da solução a longo prazo. Permite que o firewall se adapte a futuras atualizações da rede (ex: migração para 40Gbps) apenas com a troca de um módulo, em vez de todo o equipamento, promovendo economia e escalabilidade.

1.3.3.2.2. Equipamento Tipo II (Unidades Remotas de Grande Porte)

a) Requisito: Desempenho de Next Generation Firewall de 5 Gbps e 1.5 Gbps com todas as funcionalidades de segurança ativas.

Justificativa: Adequado para as maiores localidades remotas da JMU, garantindo que tenham capacidade de processamento para aplicar todas as políticas de segurança ao tráfego local e às conexões com a sede, sem comprometer a performance para os usuários.

b) Requisito: Suporte a 50.000 novas conexões/segundo e 300.000 conexões simultâneas.

Justificativa: Capacidade dimensionada para o volume de usuários e serviços dessas unidades, garantindo estabilidade e resposta rápida durante picos de uso.

1.3.3.2.3. Equipamento Tipo III (Unidades Remotas de Médio Porte)

a) Requisito: Desempenho de Next Generation Firewall de 3.2 Gbps e 1.5 Gbps com todas as funcionalidades de segurança ativas.

Justificativa: Perfil de desempenho ajustado para localidades de médio porte. Assegura a aplicação integral do mesmo nível de segurança do Data Center, porém com um hardware dimensionado para a realidade local, em conformidade com o princípio da economicidade.

b) Requisito: Suporte a 50.000 novas conexões/segundo e 300.000 conexões simultâneas.

Justificativa: Garante a fluidez e estabilidade das operações para o número de usuários e sistemas presentes nessas unidades.

1.3.3.2.4. Equipamento Tipo IV (Unidades Remotas de Pequeno Porte)

a) Requisito: Desempenho de Next Generation Firewall de 1.3 Gbps e 660 Mbps com todas as funcionalidades de segurança ativas.

Justificativa: O dimensionamento mais enxuto atende com eficiência e menor custo às necessidades das menores localidades da JMU. O mais importante é que, apesar do porte, o equipamento deve prover o conjunto completo de funcionalidades de segurança, garantindo uma postura de segurança uniforme em toda a instituição.

b) Requisito: Suporte a 20.000 novas conexões/segundo e 175.000 conexões simultâneas.

Justificativa: Capacidade suficiente para garantir a performance e a estabilidade da rede para o perfil de uso dessas unidades.

1.3.3.2.5. Especificações Técnicas de Funcionalidades (Comum a todos os equipamentos)

a) Requisito: Reconhecer pelo menos 3.000 aplicações diferentes, independente de porta e protocolo, e controlar funções específicas dentro da aplicação.

Justificativa: Essencial para implementar políticas de segurança eficazes na era da nuvem. Permite à DITIN controlar o uso de aplicações para mitigar riscos de vazamento de dados e perda de produtividade, sem precisar bloquear serviços inteiros que possam ter uso legítimo para o negócio.

b) Requisito: Possuir módulo de IPS com no mínimo 7.000 assinaturas e referência cruzada com CVE.

Justificativa: O IPS protege ativamente a rede contra tentativas de exploração de vulnerabilidades conhecidas. A referência ao CVE é crucial, pois permite correlacionar um alerta de ataque a uma vulnerabilidade específica, facilitando a gestão de riscos e a priorização de correções.

c) Requisito: Medir parâmetros de rede como jitter, perda de pacotes e latência em tempo real e redistribuir o tráfego de forma inteligente entre os links (SD-WAN).

Justificativa: Fundamental para garantir a qualidade de serviços em tempo real, como sessões de julgamento por videoconferência. O SD-WAN monitora a "saúde" dos links e desvia o tráfego crítico para o de melhor performance, garantindo uma experiência de uso fluida.

d) Requisito: Suportar VPN (Site-to-Site e Client-to-Site) com múltiplos métodos de autenticação, incluindo integração com provedores de identidade via SAML.

Justificativa: Essencial para o trabalho remoto seguro e para a interligação das unidades. O suporte a SAML é um requisito moderno que permite a implementação de Autenticação Multifator (MFA), elevando drasticamente a segurança do acesso remoto.

e) Requisito: Analisar e bloquear ameaças não conhecidas (zero-day) em tempo real, utilizando um ambiente sandbox em nuvem do próprio fabricante.

Justificativa: Malwares modernos, especialmente ransomware, são projetados para não serem detectados por assinaturas. O sandboxing analisa o comportamento do arquivo em um ambiente seguro antes que ele chegue ao usuário, sendo a defesa mais eficaz contra este tipo de ataque.

f) Requisito: Centralizar a administração de regras, políticas e logs de todos os equipamentos em uma única interface, com recursos avançados de pesquisa e correlação de eventos.

Justificativa: Indispensável para a eficiência operacional, consistência da segurança e capacidade de resposta a incidentes. Permite gerenciar dezenas de dispositivos como um só e facilita a investigação de incidentes ao consolidar e correlacionar informações de múltiplas fontes em um único local.

1.3.3.3. Requisitos de Manutenção:

A contratação prevê a prestação de Serviços Gerenciado de Segurança da Informação, o que implica que a empresa contratada será responsável pela manutenção e resolução de problemas. Os requisitos de manutenção incluem:

a) Serviços de manutenção preventiva, corretiva, adaptativa e evolutiva (melhoria funcional) para todos os equipamentos e softwares que compõem a solução, sem ônus adicional para a Contratante.

b) A forma como será conduzida a manutenção, acionamento da garantia e a comunicação entre as partes envolvidas deverão ser claramente definidas em Acordo de Nível de Serviço (SLA).

c) Resolução de qualquer problema nas licenças e serviços descritos no documento de especificação técnica.

1.3.3.4. Requisitos de projeto e de implementação:

- A Contratada será responsável por implementar e gerenciar as políticas de segurança definidas pelo cliente.
- Fornecimento de equipamentos novos e sem uso anterior.
- A solução ofertada deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta.
- O licenciamento deverá ser fornecido em sua versão mais atualizada.
- As licenças (subscrição) dos softwares que compõem os itens 1, 2, 3 e 4 do grupo 1 devem ser emitidas no nome da contratante.
- Caso seja necessário substituir licenças equivalentes durante a vigência do contrato, isso deverá ocorrer sem qualquer ônus para a contratante.
- Apoio técnico especializado nas fases de instalação, configuração, integração e ativação dos equipamentos NGFW com SD-WAN.
- Elaboração de planos de implantação e documentação técnica.
- Apoio técnico durante o período de sustentação e operação assistida da solução, com atuação pró-ativa na resolução de problemas.

1.3.3.5. Requisitos de implantação:

- O processo de disponibilização da solução em ambiente de produção deverá ser planejado em conjunto com a Contratante, minimizando impactos nas operações.
- A Contratada será responsável pela implementação e gestão das políticas de segurança, incluindo regras de firewall, IPS, Antivírus/Anti-malware, filtro URL, controle de aplicações e SD-WAN, conforme as políticas de segurança estabelecidas.
- Configuração de rotas avançadas de acordo com a demanda do cliente.
- Suporte técnico especializado para integração do equipamento para proteção de perímetro com outras soluções de segurança e redes.

1.3.3.6. Requisitos de experiência profissional

- A Contratada deverá fornecer, no mínimo, 01 (um) profissional sênior, dedicado para gerenciamento e administração de todos os serviços e equipamentos fornecidos neste edital.
- Este profissional será alocado de forma **exclusiva e contínua**, sendo responsável por atividades como apoio técnico especializado nas fases de instalação, configuração, integração e ativação; atendimento técnico dedicado de Nível 2 e 3 (troubleshooting avançado, tunning de políticas, análise de desempenho, gestão de conectividade dinâmica); elaboração de planos de implantação, documentação técnica e relatórios; suporte na criação e ajuste de políticas de segurança, regras de inspeção profunda (DPI), controle de aplicações, filtragem de conteúdo, VPNs e segmentação de tráfego via SD-WAN; e apoio técnico durante o período de sustentação e operação assistida, com atuação pró-ativa na resolução de problemas.

1.3.3.6.1. Requisitos obrigatórios para o profissional dedicado:

a) Experiência mínima de 4 (quatro) anos, comprovada, na atuação direta com soluções de NGFW, incluindo atividades de implantação, configuração, troubleshooting e suporte técnico.

- A comprovação da experiência deverá ser feita mediante apresentação de currículo atualizado e detalhado, cópias de contratos, atestados de capacidade técnica ou declarações emitidas por empresas públicas ou privadas, com descrição das atividades desempenhadas e identificação da tecnologia envolvida.

b) Conhecimento técnico avançado na solução ofertada.

c) A Contratada deverá apresentar declaração formal garantindo a alocação dedicada deste profissional durante todas as fases do projeto, inclusive suporte pós-implantação.

d) O profissional deverá estar disponível para atendimento remoto e presencial (quando necessário), respeitando os prazos de SLA definidos neste ETP.

e) O profissional técnico designado pela Contratada deverá, **sempre que solicitado pela CONTRATANTE**, realizar suas atividades de forma **presencial nas dependências da CONTRATANTE**, em **horário comercial (das 12h às 19h, em dias úteis)**, **sem quaisquer ônus adicionais** à Contratante.

f) O profissional dedicado deverá seguir todas as políticas internas de segurança da informação da Contratante.

g) A Contratante terá acesso direto ao profissional dedicado através de uma linha direta (hotline), permitindo comunicação imediata e eficaz.

Caso necessário, a Contratante poderá acionar outros recursos do suporte da contratada para a resolução de problemas.

Justificativa: A complexidade da solução de NGFW com SD-WAN e a criticidade dos serviços de segurança da informação exigem um profissional com experiência comprovada e certificações específicas do fabricante para garantir a correta implantação, configuração e sustentação, minimizando riscos operacionais e de segurança. A dedicação e o atendimento presencial garantem agilidade e proximidade com a equipe de TI da Contratante.

1.3.3.7. Requisitos de formação da equipe

Os requisitos de formação da equipe estão abrangidos nos requisitos de experiência profissional e certificações específicas exigidas para o profissional sênior dedicado[57]. A formação acadêmica e técnica específica para atuar com as tecnologias de segurança cibernética e SD-WAN é implícita nas certificações e experiência.

1.3.3.8. Acordo de Nível de Serviço (SLA)

1.3.3.8.1. Objetivo

Este Acordo de Nível de Serviço (SLA) tem como objetivo definir os níveis mínimos de desempenho, disponibilidade e qualidade para os "Serviços Gerenciados de Segurança da Informação"[1], objeto desta contratação. Ele estabelece as métricas, os tempos de resposta e solução para incidentes e requisições de serviço, bem como as penalidades aplicáveis em caso de descumprimento, assegurando que o STM receba um serviço de excelência, compatível com a criticidade de suas operações.

1.3.3.8.2. Definições

Para os fins deste SLA, aplicam-se as seguintes definições:

a) Incidente: Qualquer evento não planejado que cause, ou possa causar, uma interrupção ou redução na qualidade do serviço.

b) Requisição de Serviço: Uma solicitação formal para uma mudança padrão, como a criação de uma nova regra de firewall, a geração de um relatório específico ou uma consulta de configuração que não se origine de uma falha.

c) Horário Comercial (HC): De segunda a sexta-feira, das 09:00 às 19:00, horário de Brasília-DF, exceto feriados nacionais e do Distrito Federal.

d) Tempo de Resposta: O intervalo de tempo entre a abertura do chamado pelo STM (ou a detecção proativa pela CONTRATADA) e o início efetivo do atendimento por um analista qualificado, com a devida comunicação ao STM.

e) Tempo de Solução de Contorno: O intervalo de tempo para o restabelecimento do serviço por meio de uma solução temporária (workaround) que mitigue o impacto do incidente.

f) Tempo de Solução Definitiva: O intervalo de tempo para a resolução completa e definitiva da causa raiz do incidente.

1.3.3.8.3. Classificação de Prioridade de Incidentes

Todo incidente será classificado conforme a tabela abaixo, em comum acordo entre o STM e a CONTRATADA. Em caso de divergência, prevalecerá a classificação do STM.

Prioridade	Descrição	Exemplos
P1 - Crítica	Indisponibilidade total do serviço em um ou mais equipamentos do tipo I (Concentrador); falha que afeta a comunicação de múltiplas localidades; violação de segurança grave em andamento; indisponibilidade de sistema crítico (e-Proc/JMU) comprovadamente causada por falha na solução.	Queda completa dos firewalls da sede; falha total do acesso VPN para todos os usuários; detecção de um ataque de ransomware ativo na rede.
P2 - Alta	Degradação severa do desempenho do serviço; indisponibilidade de uma funcionalidade de segurança crítica (ex: IPS, Filtro Web); falha de um dos links gerenciados pelo SD-WAN; falha em um equipamento de localidade remota causando indisponibilidade local.	Lentidão extrema na rede afetando todos os usuários; falha no módulo de antivírus de gateway; queda de um dos links de internet da sede.
P3 - Média	Degradação parcial do serviço com baixo impacto; falha que afeta um pequeno grupo de usuários ou um serviço não crítico; falha em uma política de segurança específica.	Uma regra de firewall específica não está funcionando; falha no agendamento de um relatório; dificuldade de acesso para um único usuário.
P4 - Baixa	Incidente sem impacto perceptível no serviço; solicitação de informação ou dúvida sobre o funcionamento da solução; otimização de regra sem urgência.	Esclarecimento sobre uma funcionalidade; log de evento informativo que gerou dúvida.

1.3.3.8.4. Métricas de Nível de Serviço para Incidentes

A CONTRATADA deverá cumprir os seguintes prazos, contados a partir da abertura do chamado:

Prioridade	Canal de Acionamento	Horário de Cobertura	Tempo de Resposta (Máximo)	Tempo de Solução de Contorno (Máximo)	Tempo de Solução Definitiva (Máximo)
P1 - Crítica	Telefone (Hotline) [2] / E-mail	24x7x365	15 minutos	4 horas	24 horas
P2 - Alta	Telefone (Hotline) / E-mail	24x7x365	30 minutos	8 horas	3 dias úteis
P3 - Média	Portal Web / E-mail	Horário Comercial	1 hora	N/A	5 dias úteis
P4 - Baixa	Portal Web / E-mail	Horário Comercial	2 horas	N/A	10 dias úteis

1.3.3.8.5. Métricas de Nível de Serviço para Requisições de Serviço

Tipo de Requisição	Prazo para Conclusão (Máximo)
Alteração de política de segurança (Crítica/Emergencial)	4 horas (24x7)
Alteração de política de segurança (Padrão)	2 dias úteis
Geração de relatório customizado	3 dias úteis
Consulta técnica ou esclarecimento de dúvida	1 dia útil

1.3.3.8.6. Nível de Disponibilidade do Serviço

a) Disponibilidade Mínima Mensal: A solução, considerando os clusters de alta disponibilidade (equipamentos Tipo I), deverá ter uma disponibilidade mínima de 99,9% ao mês.

b) Cálculo da Disponibilidade: A disponibilidade será calculada pela fórmula:

Disponibilidade(%) = (1 - Tempo Total de Indisponibilidade em Minutos/Total de Minutos no Mês) X 100

c) Janelas de Manutenção: Manutenções programadas que exijam indisponibilidade do serviço deverão ser previamente acordadas com o STM com no mínimo 5 (cinco) dias úteis de antecedência e realizadas, preferencialmente, em finais de semana ou fora do horário de expediente. Janelas de manutenção acordadas não serão computadas como tempo de indisponibilidade.

1.3.3.8.7. Penalidades por Descumprimento do SLA

Infração	Percentual de Glosa
Descumprimento do Tempo de Resposta (P1 ou P2)	2% por evento
Descumprimento do Tempo de Solução de Contorno (P1)	5% por evento, por hora de atraso
Descumprimento do Tempo de Solução de Contorno (P2)	3% por evento, por hora de atraso
Disponibilidade Mensal entre 99,0% e 99,89%	10%
Disponibilidade Mensal entre 98,0% e 98,99%	15%
Disponibilidade Mensal abaixo de 98,0%	20%

- **Limite de Glosa:** O somatório das glosas aplicadas em um mês não poderá exceder 30% do valor da fatura mensal. A reincidência contumaz no descumprimento do SLA poderá ensejar a abertura de processo administrativo para rescisão contratual por inexecução.

1.3.3.8.8. Relatórios de Nível de Serviço

A CONTRATADA deverá fornecer ao STM, até o 5º dia útil de cada mês, um relatório detalhado contendo o desempenho do serviço no mês anterior. O relatório deve incluir, no mínimo:

a) Lista de todos os incidentes e requisições de serviço, com seus respectivos horários de abertura, resposta e solução.

b) Cálculo do cumprimento de todas as métricas de SLA.

c) Cálculo da disponibilidade mensal do serviço.

d) Análise de causa raiz para todos os incidentes de prioridade P1 e P2.

e) Sumário executivo das atividades realizadas pelo profissional dedicado.

1.3.3.9. Requisitos Temporais:

A prestação de serviços e a garantia dos equipamentos deverão ser pelo período de 60 meses.

O contrato vigente encerra-se em dezembro de 2025, sendo crucial que a nova contratação esteja operacional a partir de janeiro de 2026 para garantir a continuidade dos serviços de proteção de perímetro.

1.3.3.10. Requisitos de Segurança da Informação

A CONTRATADA deverá assinar Termo de Sigilo/Confidencialidade, obrigando-se a não realizar, promover, nem incentivar a divulgação de qualquer dado ou informação do ambiente computacional do STM, bem como dos dados ou informações contidas nele sem a prévia autorização.

Os encarregados dos serviços previstos nas respectivas Ordens de Serviço deverão assinar Termo de Confidencialidade antes de iniciar suas atividades junto ao STM.

Observar normativos e todos os procedimentos de segurança necessários e definidos na legislação pertinente e vigente no Poder Judiciário.

Submeter seus recursos técnicos aos regulamentos de segurança e disciplina instituídos pelo ÓRGÃO, durante o tempo de permanência nas suas dependências.

Disponibilizar links seguros para a realização de trabalho remoto, quando couber.

A solução deve prover a segurança cibernética e proteção de dados, conforme recomendações da Política de Segurança Cibernética da JMU e Resolução CNJ nº 396/2021.

Integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede.

1.3.3.11. Requisitos Sociais, Ambientais e Culturais

A CONTRATADA deverá tomar conhecimento do Plano de Logística Sustentável PLS, das Orientações do Controle Interno e demais procedimento do STM, ainda que a natureza dos serviços não se aplique, devidamente justificada pela inexistência de produtos ou atividades que se enquadrem nas condições exigidas nos critérios de Sustentabilidade Ambiental, Social e Econômica.

1.3.3.12. Requisitos Legais

A solução deve estar em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709, de 14 de agosto de 2018.

A solução deve atender aos requisitos para o atendimento do protocolo para investigação de ilícitos cibernéticos, conforme os requisitos mínimos de segurança definidos na Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética no âmbito do Poder Judiciário.

1.3.3.13. Demais Requisitos Aplicáveis

Garantir prazos de entrega a fim de evitar penalidades por atrasos.

Desenvolver as atividades necessárias mediante trabalho híbrido (remoto/presencial/híbrido) e nos termos dos padrões de segurança e integridade previstas pelo Poder Judiciário e pelo STM.

A Contratada deverá estar apta a abrir e receber Ordens de Serviço via correio eletrônico, sistema específico de controle de demandas ou, página na internet (WEB) dedicada, em regime 24x7 (24 horas por dia, em todos os sete dias da semana).

Responsabilizar-se pelos materiais, produtos, ferramentas, instrumentos e equipamentos disponibilizados para a execução dos serviços, sejam eles prestados remotamente ou nas instalações do STM, não cabendo ao STM qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer.

Promover o afastamento, no prazo máximo de 24 (vinte e quatro) horas após o recebimento da notificação por ofício ou e-mail, de qualquer dos seus recursos técnicos que não correspondam aos critérios de confiança ou que perturbem a ação da equipe de fiscalização do STM.

1.3.3.14. Verificação de Amostra do Objeto

A possibilidade de verificação de amostra, tem previsão no artigo 17, §3º, artigo 41, inciso II, e artigo 42, §2º, todos da Lei nº 14.133, de 2021, e no artigo 12, § 1º da IN SGD/ME nº 94, de 2022. Portanto, como são equipamentos de altos valores, o STM poderá solicitar amostra se assim desejar.

Para fins de aceitação pelo STM, este Órgão poderá solicitar amostra para aferir as funcionalidades dos equipamentos em testes de bancada. Os itens de performance serão comprovados mediante datasheet ou declaração do fabricante em casos excepcionais. Os testes de bancada são destinados, exclusivamente, a dirimir dúvidas dos demais participantes do certamente licitatório, quando suscitadas, sobre as capacidades dos equipamentos que serão entregues pelo participante vencedor do certame. Os testes de bancadas consistirão em:

Aferição da capacidade de throughput de tráfego descriptografado pelo equipamento a ser testado.

Aferição da capacidade de trhoughput de inspeção de tráfego SSL do equipamento a ser testado.

Aferição das especificações técnicas (portas de comunicação, capacidade de processamento, memórias estáticas e volátil) do equipamento a ser testado.

Capacidades do software do equipamento a ser testado.

1.3.4. Aderência a padrões e modelos

1.3.4.1. Modelo Nacional de Interoperabilidade - MNI

Aplicabilidade e Justificativa: A aderência é indireta, porém fundamental. O firewall não processa mensagens MNI, mas cria o ambiente seguro e os canais de comunicação confiáveis para que os sistemas finalísticos da JMU (e-Proc) possam trocar informações com outros órgãos de forma segura, habilitando e protegendo a interoperabilidade exigida pelo CNJ.

1.3.4.2. Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil

Aplicabilidade e Justificativa: A aderência é direta e mandatória. A solução deverá ser plenamente compatível com certificados digitais emitidos sob a hierarquia da ICP-Brasil, que são indispensáveis para as funcionalidades de VPN e inspeção de tráfego SSL, garantindo a autenticidade e a confidencialidade nas comunicações eletrônicas, conforme as exigências legais para o processo judicial eletrônico.

1.3.4.3. Modelo de Requisitos MoReq-Jus

Aplicabilidade e Justificativa: A aderência é de natureza indireta, mas crítica. A solução de NGFW é um dos principais controles que garantem a proteção dos sistemas de gestão documental (SEI) e processual (e-Proc) contra acessos não autorizados e ataques. Ao assegurar a integridade da infraestrutura, a solução de segurança é um pilar que sustenta a conformidade do órgão com as diretrizes do MoReq-Jus.

1.4. Atendimento da demanda

Esta seção analisa as diferentes possibilidades para o atendimento da necessidade do STM, avaliando alternativas de solução, modelos de contratação e a capacidade do mercado de prover o objeto licitatório.

1.4.1. Portal do Software Público Brasileiro

Análise: Foi realizada uma análise no Portal do Software Público Brasileiro em busca de soluções que pudessem atender à demanda.

Conclusão: Dada a natureza da contratação, que envolve o fornecimento de equipamentos de hardware altamente especializados (NGFW), licenciamento de software proprietário de segurança e, principalmente, a prestação de um serviço gerenciado contínuo com alocação de profissional, não foram encontradas soluções aderentes no Portal. As soluções disponíveis no portal são, em sua maioria, softwares de aplicação e gestão, não abrangendo a complexidade de hardware e serviços de segurança de perímetro exigidos.

1.4.2. Análise Comparativa de Soluções de TIC

Para atender à necessidade de modernização e gestão da segurança de perímetro, foram consideradas as seguintes alternativas de solução:

Solução 1: Aquisição Direta dos Equipamentos e Suporte Básico do Fabricante

Descrição: Neste modelo tradicional, o STM realizaria a compra dos equipamentos (NGFW), tornando-os ativos da instituição. A contratação se resumiria ao fornecimento do hardware e de um pacote de suporte técnico padrão do fabricante (ex: 8 horas por dia, 5 dias por semana, com troca de peças no próximo dia útil). Toda a gestão, monitoramento, configuração de políticas e resposta a incidentes seriam de responsabilidade exclusiva da equipe interna da DITIN.

Vantagens: Propriedade plena dos ativos; potencial menor custo de desembolso inicial se comparado ao serviço gerenciado.

Desvantagens: Exigiria uma equipe interna maior e altamente especializada para operar a solução 24x7, o que vai de encontro a uma fraqueza já diagnosticada no PDTIC/JMU de "Equipe insuficiente para o quantitativo de demandas de TIC". A responsabilidade por todo o ciclo de vida do gerenciamento de incidentes recairia sobre o STM, sem a garantia de monitoramento contínuo fora do horário comercial, o que representa um risco elevado para a segurança da instituição.

Solução 2: Contratação de Serviço Gerenciado de Segurança (Modelo Proposto)

Descrição: Este é o modelo detalhado neste ETP. Uma empresa especializada é contratada para fornecer uma solução completa, que inclui os equipamentos (em regime de comodato ou como parte integrante do serviço), as licenças, o suporte técnico, e, crucialmente, o serviço de gerenciamento contínuo. Este serviço engloba monitoramento 24x7 por um SOC/NOC, gestão de políticas, resposta a incidentes, relatórios e a alocação de um profissional sênior dedicado ao ambiente do STM.

Vantagens: Acesso imediato a expertise de alto nível; garantia de monitoramento e resposta a incidentes 24x7; alivia a carga operacional da equipe interna, permitindo foco em atividades estratégicas; transferência de parte do risco operacional para a contratada; custos mensais previsíveis (OPEX). Atende plenamente aos requisitos de negócio e técnicos da demanda.

Desvantagens: O custo recorrente pode ser superior ao do modelo de aquisição direta, embora o custo total de propriedade (TCO), ao incluir os custos de pessoal interno necessário no primeiro modelo, possa ser mais vantajoso.

Solução 3: Adoção de uma Arquitetura SASE (Secure Access Service Edge)

Descrição: Modelo nativo em nuvem onde a segurança de rede e o acesso são fornecidos como um serviço de um provedor de nuvem. Minimiza a necessidade de hardware local, focando em políticas de segurança que seguem o usuário onde quer que ele esteja.

Vantagens: Altamente escalável; modelo de segurança moderno e alinhado ao trabalho remoto; potencial simplificação da gestão.

Desvantagens: Representaria uma mudança arquitetônica drástica e de alta complexidade para a rede da JMU. A maturidade e a oferta de soluções SASE completas no âmbito do setor público brasileiro ainda são limitadas. Poderiam surgir questões de soberania e residência de dados, que são extremamente sensíveis para um órgão do Poder Judiciário. A migração seria um projeto de longo prazo e com riscos de implementação mais elevados do que a modernização da arquitetura atual.

Conclusão da Análise: A Solução 2 (Serviço Gerenciado) é a que melhor atende às necessidades do STM, pois resolve o problema técnico da segurança de perímetro e, ao mesmo tempo, supre a necessidade de pessoal especializado para a gestão contínua, mitigando o risco identificado da insuficiência de equipe interna.

1.4.3. Contratações Públicas Similares

Como parte da fase de pesquisa de preços e elaboração do Termo de Referência, será realizada uma ampla pesquisa no Painel de Preços do Governo Federal, no Portal Nacional de Contratações Públicas (PNCP) e por meio de contato direto com outros órgãos do Poder Judiciário (como CNJ, tribunais superiores e federais) para identificar contratações similares. O objetivo é analisar os modelos adotados, os fornecedores contratados e os valores praticados, a fim de balizar e validar a vantajosidade da presente contratação.

1.4.4. Soluções similares em outros órgãos

A demanda por serviços gerenciados de segurança, incluindo NGFW com SD-WAN, é uma prática consolidada em diversas esferas da administração pública brasileira, servindo como referência para novas contratações. A análise de processos licitatórios recentes demonstra a adoção de modelos e especificações técnicas similares por uma vasta gama de entidades, validando a abordagem e os requisitos do mercado.

Órgãos de Controle e Judiciário: O Tribunal de Contas do Estado de Santa Catarina (TCE/SC), através do Pregão Eletrônico nº 38/2024, contratou a "prestação de serviços de locação de firewall para Segurança da Informação de perímetro", um modelo focado em despesa operacional (OpEx).

Poder Legislativo: A Assembleia Legislativa do Estado de Goiás (ALEGO) realizou a contratação para a "Renovação da Subscrição da Licença" de seus equipamentos NGFW existentes, garantindo a continuidade do suporte e das atualizações de segurança.

Administração Federal: O Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) licitou a "subscrição das licenças de uso de software gerenciador do Firewall" para seus equipamentos, e o Ministério da Gestão e da Inovação (MGI) lançou a Consulta Pública nº 9/2025 para uma contratação centralizada de soluções NGFW para toda a Administração Pública Federal, visando padronização e economia de escala. A

Controladoria-Geral da União (CGU) também figura entre os órgãos que demandam esse tipo de solução.

Empresas Estatais: A Companhia de Processamento de Dados do Estado da Bahia (PRODEB) conduziu uma licitação de grande vulto (Pregão Eletrônico nº 006/2024) para o fornecimento de um conjunto abrangente de soluções de segurança, incluindo NGFW e serviços gerenciados.

Instituições de Ensino: O Instituto Federal do Ceará (IFCE) firmou o Contrato 11/2022 para um "serviço gerenciado de segurança da informação de forma remota".

Segurança Pública: A Polícia Civil do Governo do Estado de Rondônia licitou uma solução integrada de NGFW com SD-WAN para proteger todo o seu parque tecnológico.

Administração Municipal: Prefeituras como as de Pedro Leopoldo/MG ,

Contagem/MG e Itajaí/SC demonstraram alta maturidade técnica ao publicar editais com requisitos detalhados para plataformas integradas de NGFW/SD-WAN com serviços gerenciados, evidenciando que a necessidade de proteção avançada de perímetro é uma preocupação em todos os níveis de governo.

Esses exemplos demonstram um padrão de mercado claro, com foco em serviços gerenciados, funcionalidades integradas de NGFW e SD-WAN, e modelos contratuais que privilegiam a continuidade e a transferência de risco operacional para o fornecedor.

1.4.5. Modelos de Aquisição/Prestação do Serviço

Conforme a análise de soluções, o modelo de prestação de serviço escolhido é o de **Serviço Gerenciado de Segurança**, com duração prevista de 60 meses. A remuneração se dará por meio de pagamento mensal recorrente, caracterizando a despesa como custo operacional (OPEX). Este modelo foi selecionado por ser o mais completo, englobando não apenas a tecnologia, mas a camada de inteligência, gestão e suporte especializado, que é o núcleo da necessidade do STM.

1.4.6. Contratações correlatas e/ou interdependentes

A execução desta contratação possui interdependência com os seguintes serviços e infraestruturas já existentes no STM:

- **Links de Comunicação:** A solução de SD-WAN irá gerenciar os links de internet e comunicação de dados já contratados pelo STM. A performance do serviço depende da qualidade desses links.
- **Infraestrutura de Rede Interna:** Os equipamentos serão conectados à infraestrutura de switches e cabeamento do STM. A compatibilidade e o bom funcionamento dessa infraestrutura são essenciais.
- **Sistema de Autenticação:** A solução se integrará ao Microsoft Active Directory do STM para a identificação de usuários e aplicação de políticas, sendo dependente da disponibilidade deste serviço.

Não há necessidade de outras contratações prévias para viabilizar este projeto. No entanto, o sucesso desta contratação é um pilar para a segurança de todas as demais soluções e sistemas de TIC da JMU.

1.5. Análise dos Custos Totais da Demanda

Para a estimativa de custos da contratação, foram solicitadas e recebidas propostas de cinco empresas especializadas no setor: Compwire, ENQ Soluções, Global IP, Wise IT e Yssy Soluções. As propostas contemplam o fornecimento da solução completa de Serviço Gerenciado de Segurança, incluindo todos os equipamentos, licenças e serviços para o período de 60 (sessenta) meses.

A análise comparativa dos custos totais apresentados nas propostas comerciais é detalhada abaixo:

Empresa	Valor Total para 60 Meses (R$)
Yssy Soluções	R$9.927.840,00
Global IP	R$11.447.334,35
ENQ Soluções	R$11.965.200,00
Compwire	R$12.243.000,00

Wise IT	R$12.653.150,40
Média	**R$11.647.304,95**

Com base na média dos valores obtidos nas cotações, o valor total estimado para a presente contratação **é de R$ 11.647.304,95 (onze milhões, seiscentos e quarenta e sete mil, trezentos e quatro reais e noventa e cinco centavos)** para o período de 60 meses.

A seguir, a estimativa detalhada com os custos unitários médios, calculados a partir das propostas recebidas, que servirão de referência para o certame licitatório.

1.6. Escolha e Justificativa da Solução

Com base na análise das necessidades do Superior Tribunal Militar (STM) e nas diferentes alternativas de mercado investigadas na seção 1.4 deste documento, esta seção formaliza a escolha da solução mais adequada e apresenta as justificativas técnicas e estratégicas para essa decisão.

1.6.1. Descrição da Solução Escolhida

Solução Escolhida: Contratação de Serviço Gerenciado de Segurança da Informação (MSS - *Managed Security Service*), composta por equipamentos de proteção de perímetro do tipo NGFW com SD-WAN, licenciamento, suporte e garantia pelo período de 60 meses.

Descrição Detalhada: A solução escolhida não se trata de uma simples aquisição de equipamentos, mas sim de um serviço completo e contínuo. Este modelo prevê que a empresa CONTRATADA será responsável por todo o ciclo de vida da segurança de perímetro, incluindo:

O fornecimento dos equipamentos (NGFW) adequados para cada localidade da JMU, em regime de comodato ou como parte integrante do serviço.

O fornecimento de todas as licenças de software (subscrições) necessárias para a operação das funcionalidades de segurança avançada.

A implantação, configuração e otimização contínua da solução.

O monitoramento proativo de segurança e desempenho, 24 horas por dia, 7 dias por semana, por meio de um Centro de Operações de Segurança (SOC/NOC).

A alocação de um profissional sênior, certificado e com dedicação exclusiva ao ambiente do STM, para atuar como ponto focal técnico, garantindo agilidade e expertise no suporte avançado e na gestão estratégica da solução.

Motivação e Justificativa da Escolha: A escolha por um Serviço Gerenciado, em detrimento da aquisição direta dos ativos, é estrategicamente mais vantajosa para o STM. Conforme diagnosticado no PDTIC/JMU, a "Equipe insuficiente para o quantitativo de demandas de TIC" é uma fraqueza institucional. O modelo de serviço gerenciado supre diretamente essa carência, agregando uma camada de especialistas à equipe do STM sem a necessidade de novas contratações de pessoal. Ele transfere o risco operacional da gestão diária da segurança para a CONTRATADA, permitindo que a equipe interna da DITIN se concentre em atividades mais estratégicas de governança e segurança da informação. Adicionalmente, este modelo garante o acesso contínuo a tecnologias de ponta e a expertise de mercado, com custos operacionais previsíveis (OPEX), o que se alinha aos princípios de eficiência e economicidade.

1.6.2. Benefícios Esperados

A implementação da solução escolhida trará os seguintes benefícios para a Justiça Militar da União:

- **Eficácia:** Elevação drástica da postura de segurança cibernética, com proteção eficaz contra ameaças modernas como ransomware e ataques de dia-zero. Maior capacidade de atender e comprovar a conformidade com normativos como a ENSEC-PJ e a Lei Geral de Proteção de Dados (LGPD).
- **Eficiência:** Resposta a incidentes de segurança significativamente mais rápida devido ao monitoramento 24x7 e ao suporte especializado. Otimização do uso e da resiliência dos links de comunicação através da tecnologia SD-WAN. Liberação da força de trabalho interna para atividades de maior valor agregado.
- **Economicidade:** Previsibilidade de custos com um valor mensal fixo pelo serviço. Mitigação do risco financeiro associado a um incidente de segurança de grande porte. Eliminação da necessidade de grandes investimentos de capital (CAPEX) para a renovação do parque tecnológico de segurança.
- **Padronização:** Implementação de uma plataforma de segurança única e centralmente gerenciada, garantindo a aplicação consistente de políticas de segurança em todas as localidades da JMU, da sede às auditorias mais remotas.

1.6.3. Resultados Esperados

Conforme o Documento de Oficialização da Demanda (DOD), espera-se alcançar os seguintes resultados:

- **Aprimoramento da Segurança Cibernética:** Redução da vulnerabilidade a ataques virtuais complexos e proteção eficaz dos dados e sistemas da JMU.
- **Otimização da Prestação de Serviços:** Manutenção da disponibilidade e estabilidade dos serviços online, com resolução ágil de problemas técnicos.
- **Suporte Técnico Especializado e Eficaz:** Acesso a profissionais certificados e experientes para a resolução rápida e precisa de incidentes de segurança e problemas técnicos.
- **Continuidade e Estabilidade dos Serviços:** Minimização de interrupções e da indisponibilidade de sistemas, garantindo a continuidade das atividades da JMU.
- **Modernização do Parque Tecnológico:** Manutenção de um parque tecnológico de segurança atualizado com as últimas tecnologias disponíveis, melhorando a resposta contra ataques virtuais.

1.6.4. Relação entre a Demanda Prevista e a Quantidade de Bens e/ou Serviços Contratados

A quantidade de equipamentos e serviços foi dimensionada para atender às necessidades de todas as localidades da Justiça Militar da União, garantindo cobertura completa e adequada ao porte de cada unidade.

Item	Descrição do Serviço/Equipamento	Unidade	Quantidade	Justificativa da Quantidade
1	Serviço composto por equipamento NGFW com SD-WAN - **Tipo I (Concentrador)**	Unidade	2	Destinados ao Data Center da Sede do STM, para operar em um cluster de Alta Disponibilidade (Ativo/Passivo), garantindo redundância e continuidade em caso de falha de um dos equipamentos.
2	Serviço composto por equipamento NGFW com SD-WAN - **Tipo II (Unidades Remotas)**	Unidade	1	Para atender à auditoria remota de maior porte da JMU, com maior número de usuários e volume de tráfego.
3	Serviço composto por equipamento NGFW com SD-WAN - **Tipo III (Unidades Remotas)**	Unidade	3	Para atender às auditorias remotas de médio porte, dimensionadas conforme a estrutura e necessidade dessas localidades.
4	Serviço composto por equipamento NGFW com SD-WAN - **Tipo IV (Unidades Remotas)**	Unidade	12	Para atender às auditorias remotas de menor porte, garantindo o mesmo nível de segurança com um equipamento de custo e performance adequados à sua demanda.
5	Serviço composto por **Gerência centralizada, logs, eventos e relatórios**	Unidade	1	Um único serviço de gerenciamento centralizado é necessário para administrar, monitorar e correlacionar os eventos de todos os 18 equipamentos (2+1+3+12), garantindo visibilidade unificada e consistência nas políticas.

1.6.5. Estimativa do Custo Total da Solução Escolhida

A estimativa de valor para a presente contratação, apresentada a seguir, foi calculada com base nos preços e condições comerciais obtidos em ampla pesquisa de mercado, da qual resultaram 5 (cinco) propostas formais. Tais propostas, fornecidas pelas empresas Compwire , ENQ Soluções , Global IP , Wise IT e Yssy Soluções , constam em anexo a este Estudo Técnico Preliminar e servem como documento de suporte para os valores referenciais.

A memória de cálculo para a definição dos valores de referência consistiu na apuração da média aritmética dos preços unitários mensais para cada um dos itens que compõem o objeto, conforme os valores apresentados nas propostas coletadas. Este método assegura uma estimativa fidedigna e alinhada às práticas de mercado para a solução pretendida.

A tabela abaixo detalha o valor estimado da contratação, consolidando os quantitativos necessários, os preços unitários de referência e o valor total projetado para a vigência de 60 (sessenta) meses.

Item	Descrição	Quantidade Total	Valor Unitário Mensal Estimado (R$)	Valor Total Estimado para 60 meses (R$)
1	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo I (Concentrador)	2	R$35.892,80	R$4.307.136,00
2	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-	1	R$4.064,10	R$243.846,00

	WAN - Tipo II (Unidades Remotas)			
3	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN-Tipo III (Unidades Remotas)	3	R$3.214,28	R$578.570,40
4	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo IV (Unidades Remotas)	12	R$2.455,95	R$1.768.284,00
5	Serviço composto por Gerência centralizada, logs, eventos e relatórios para equipamentos de proteção de perímetro com SD-WAN.	1	R$79.157,84	R$4.749.470,40
	Valor Total Estimado da Contratação			R$11.647.306,80

Observação: O valor total estimado calculado pela média dos preços unitários (R$ 11.647.306,80) apresenta uma pequena diferença em relação à média dos valores totais das propostas (R$ 11.647.304,95) devido aos arredondamentos nos cálculos individuais por item. Ambas as cifras confirmam a faixa de preço esperada para a contratação.

1.7. Declaração de viabilidade da contratação

Com base em todos os estudos e análises realizados e documentados nas seções anteriores deste Estudo Técnico Preliminar, a equipe de planejamento da contratação declara:

Declaração de Viabilidade: **VIÁVEL**

Justificativa:

A contratação é declarada viável pelas seguintes razões, que consolidam os achados deste estudo:

- Alinhamento Estratégico Robusto: A demanda está em plena conformidade com os planejamentos de mais alto nível da instituição. Alinha-se diretamente ao
- Planejamento Estratégico da JMU (PE-JMU 2021-2026), especificamente nos objetivos de "Fortalecer a governança e a segurança de dados e informações" e "Otimizar a infraestrutura e as soluções de TIC". Adicionalmente, atende a múltiplos objetivos do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC 2025-2026), em especial os de "Aprimorar a Segurança da Informação e a Gestão de Dados" e "Promover Serviços de Infraestrutura e Soluções Corporativas". A contratação também é aderente às estratégias nacionais do Poder Judiciário, como a ENTIC-JUD e a ENSEC-PJ.
- Necessidade Crítica e Inadiável: A modernização da segurança de perímetro é uma necessidade crítica para proteger os ativos de informação da JMU contra ameaças cibernéticas cada vez mais complexas e para garantir a continuidade dos serviços jurisdicionais. A não realização desta contratação exporia a instituição a riscos operacionais, financeiros e de reputação inaceitáveis.
- Solução Adequada e Vantajosa: A análise de alternativas demonstrou que o modelo de Serviço Gerenciado de Segurança é o mais adequado para a realidade do STM. Ele não apenas supre as necessidades tecnológicas com equipamentos de ponta, mas também resolve a carência de pessoal especializado para a gestão 24x7, um ponto fraco institucional identificado. Esta abordagem se mostra mais eficaz e com melhor custo-benefício em longo prazo do que a simples aquisição de ativos.
- Viabilidade de Mercado: A prospecção inicial indica que o mercado de TIC no Brasil possui plena capacidade de atender aos requisitos da contratação. Existe um número suficiente de fornecedores de tecnologia e de empresas prestadoras de serviço com a qualificação necessária para garantir uma ampla competitividade no certame.

Em conclusão, a contratação é tecnicamente possível, estrategicamente alinhada, e os resultados e benefícios esperados, como a drástica redução de riscos e o aumento da estabilidade e segurança dos serviços, justificam plenamente o investimento a ser realizado.

2. CAPÍTULO 2: SUSTENTAÇÃO DO CONTRATO

2.1. Adequação do Ambiente

A implantação da solução de segurança gerenciada exige a avaliação e a garantia de condições adequadas no ambiente de TIC do STM e das demais localidades da Justiça Militar da União (JMU). As seguintes adequações e preparativos são necessários:

a) Infraestrutura Tecnológica:

- Espaço em Rack: Será necessário garantir espaço físico disponível em racks de 19 polegadas para a instalação dos equipamentos em todas as 17 localidades (Sede e 16 Auditorias). Na Sede do STM, deverão ser disponibilizadas 2U de espaço para a instalação do cluster de alta disponibilidade (equipamentos Tipo I).
- Conectividade de Rede: É preciso assegurar a disponibilidade de portas de rede (cobre e fibra óptica, conforme a especificação de cada equipamento) nos switches para a conexão das novas soluções de NGFW. A equipe de infraestrutura da DITIN deverá prover o cabeamento necessário para interligar os novos equipamentos ao core da rede e aos links de comunicação.
- Planejamento de Endereçamento IP: A Coordenadoria de Infraestrutura de Tecnologia (COTEC) será responsável por planejar e alocar os endereços IP necessários para as interfaces de gerenciamento, dados e sincronismo de todos os novos equipamentos.

b) Infraestrutura Elétrica:

- Pontos de Energia: Deverão ser disponibilizados pontos de energia elétrica estabilizada (conectados a no-breaks e, preferencialmente, a circuitos elétricos distintos para equipamentos com fontes redundantes) em quantidade suficiente para todos os novos equipamentos em cada localidade. Para os equipamentos Tipo I na Sede, que possuem fontes redundantes, serão necessários no mínimo 2 (dois) pontos de energia para cada equipamento.
- Capacidade Elétrica e de Climatização: A carga elétrica adicional e a dissipação de calor dos novos equipamentos são consideradas marginais e compatíveis com a capacidade de energia e climatização existentes no Data Center do STM e nas salas técnicas das Auditorias.

c) Logística de Implantação:

- Planejamento de Migração: A substituição dos equipamentos de segurança atuais pelos novos é uma atividade de alta criticidade. Será elaborado um Plano de Migração em conjunto com a futura CONTRATADA, detalhando todas as etapas do processo.
- Janela de Manutenção: A efetiva migração do tráfego para a nova solução (operação de cutover) será realizada em janelas de manutenção programadas, preferencialmente em fins de semana ou em horários de baixo expediente, para minimizar o impacto sobre os serviços jurisdicionais e administrativos. A comunicação sobre a janela será feita com a devida antecedência a todas as partes interessadas.
- Acesso Físico: O STM garantirá o acesso seguro dos técnicos da CONTRATADA às suas dependências para a instalação física dos equipamentos, mediante agendamento e acompanhamento pela equipe da DITIN.

d) Espaço Físico e Mobiliário:

- Não há necessidade de aquisição de novo mobiliário para a execução deste contrato. O STM disponibilizará uma estação de trabalho temporária (mesa, cadeira e ponto de rede) para o profissional dedicado da CONTRATADA durante as visitas ou períodos de trabalho presencial nas dependências do Tribunal, quando solicitado.

e) Impacto Ambiental:

- Equipamentos Novos: Espera-se que os novos equipamentos, por serem de tecnologia mais recente, possuam maior eficiência energética em comparação com os equipamentos a serem substituídos, o que pode representar um impacto ambiental positivo pela redução no consumo de energia.
- Descarte de Equipamentos: O descarte dos equipamentos de segurança que serão descomissionados será realizado pela empresa do contrato atual, tendo em vista o equipamento pertencer à contratada.

2.2. Recursos Materiais e Humanos

Recursos Materiais:

Não foi identificada a necessidade de realizar outras contratações de recursos materiais que sejam pré-requisito para esta. A solução a ser contratada é completa e autossuficiente, incluindo todos os equipamentos de hardware, software e licenças necessários para sua operação. A sua implementação dependerá da infraestrutura de rede e elétrica já existente e funcional do STM, conforme detalhado no item 2.1.

Recursos Humanos:

- **Pessoal para Operação do Serviço:** O modelo de Serviço Gerenciado foi escolhido justamente para suprir a necessidade de recursos humanos especializados na operação diária da solução. Portanto, o pessoal técnico para o monitoramento 24x7 e a gestão de incidentes será de responsabilidade da CONTRATADA, incluindo o profissional sênior dedicado, que é um requisito chave desta contratação.
- **Equipe de Gestão e Fiscalização do Contrato (STM):** Para a correta gestão e fiscalização do contrato, o STM designará servidores da sua equipe técnica que atuarão como fiscais do contrato. As habilidades mínimas necessárias para essa equipe interna são:

Gestor do Contrato: Conhecimento em gestão e fiscalização de contratos de TIC, com capacidade para interpretar e fazer cumprir as cláusulas contratuais e os Acordos de Nível de Serviço (SLA).

Equipe Técnica de Apoio: Conhecimento em redes de computadores e segurança da informação para avaliar tecnicamente os relatórios mensais entregues pela CONTRATADA, validar a pertinência das configurações aplicadas, interagir com o profissional dedicado para discutir melhorias e validar a resolução de incidentes complexos.

- **Capacitação:** Para garantir a eficácia da fiscalização e o máximo aproveitamento da solução contratada, é fundamental que a equipe técnica do STM receba treinamento da CONTRATADA.

  Necessidade: Exige-se que a CONTRATADA forneça um treinamento oficial ou customizado para, no mínimo, 5 (cinco) técnicos da equipe da DITIN.

  Objetivo do Treinamento: A capacitação deverá abranger, no mínimo, a arquitetura da solução implementada, o uso da console de gerenciamento em modo de visualização (*read-only*), a geração e interpretação de relatórios de segurança e desempenho, e os procedimentos para abertura e acompanhamento de chamados.

  Justificativa: Este treinamento não visa formar operadores, mas sim **fiscais e gestores qualificados**. Ele capacitará a equipe do STM a auditar o trabalho da CONTRATADA, compreender os relatórios de SLA, dialogar tecnicamente com o provedor de serviço e identificar proativamente oportunidades de melhoria na segurança, em total alinhamento com o Objetivo Estratégico OE7 do PDTIC/JMU: "Reconhecer e Desenvolver as Competências dos Colaboradores da TIC".

2.3. Continuidade do Fornecimento

Este item aborda o planejamento e as estratégias para assegurar a continuidade do fornecimento do serviço, dada a sua natureza crítica e permanente para as operações da Justiça Militar da União (JMU).

a) Natureza da Necessidade: O serviço de proteção de perímetro é de natureza contínua e essencial. A segurança da informação não é um projeto com início, meio e fim, mas um processo ininterrupto e vital para a proteção dos dados e a disponibilidade dos sistemas da JMU. A interrupção deste serviço não é uma opção aceitável.

b) Efeitos de uma Descontinuidade: Uma eventual interrupção do serviço de NGFW gerenciado teria um impacto catastrófico e imediato sobre todas as atividades do STM e das Auditorias. Os efeitos incluem:

- **Paralisação da Prestação Jurisdicional Eletrônica:** Indisponibilidade total de sistemas críticos como o e-Proc/JMU para o público externo (advogados, partes) e para o trabalho interno.
- **Interrupção da Comunicação Externa:** Perda completa do acesso à internet para todos os usuários, inviabilizando pesquisas, comunicações por e-mail e acesso a serviços externos.
- **Isolamento das Unidades Remotas:** Falha na comunicação via SD-WAN entre a Sede e as 16 Auditorias, impedindo a troca de informações e o acesso a sistemas centralizados.
- **Inviabilização do Trabalho Remoto:** O serviço de VPN deixaria de funcionar, impedindo o acesso seguro de magistrados e servidores que estiverem em regime de teletrabalho.
- **Exposição Crítica a Ameaças**: A desativação do firewall removeria a principal camada de defesa da rede, deixando a infraestrutura interna do STM exposta e altamente vulnerável a ataques cibernéticos.

c) Hipóteses de Interrupção Contratual:

- **Falha Técnica Grave:** Incidente técnico de grande porte na solução que a CONTRATADA não consiga resolver dentro dos prazos do SLA.
- **Falha Operacional da CONTRATADA:** Incapacidade da empresa em prestar o serviço por problemas em sua própria estrutura (ex: falência, perda de pessoal chave, desativação do SOC/NOC).
- **Término do Contrato sem Sucessor**: Falha no processo administrativo do STM em concluir uma nova licitação a tempo do término do contrato de 60 meses.

d) Estratégias para Garantir a Continuidade:

- Mecanismos de Prevenção Contratual: O contrato a ser firmado deverá conter cláusulas que mitiguem os riscos de interrupção, como:
  - **SLA Robusto:** Acordo de Nível de Serviço com penalidades significativas, conforme detalhado na proposta de SLA, que desestimulem a má prestação do serviço.
  - **Exigência de Backup das Configurações:** A CONTRATADA será obrigada a fornecer ao STM, trimestralmente ou sempre que houver alteração relevante, um backup completo e atualizado de todas as configurações da solução. Este backup é um ativo estratégico que facilitará a migração para um novo provedor ou plataforma em caso de necessidade.
  - **Plano de Continuidade da Contratada:** Será exigido que a licitante apresente seu Plano de Continuidade de Negócios (PCN), demonstrando como ela própria manteria a prestação do serviço ao STM em caso de desastres em sua própria infraestrutura.
  - **Planejamento Administrativo para Sucessão do Contrato:** Esta é a principal estratégia interna do STM. A área administrativa, em conjunto com a DITIN, deverá iniciar os procedimentos para a nova contratação com uma antecedência mínima de 24 (vinte e quatro) meses antes do término da vigência de 60 meses do contrato. Este prazo é necessário para cobrir todas as etapas de um processo licitatório de alta complexidade (planejamento, ETP, termo de referência, licitação, homologação) sem risco de descontinuidade do serviço.

2.4. Transição Contratual e encerramento do contrato.

As seguintes atividades e regras deverão ser obrigatoriamente observadas pela CONTRATADA no período de transição, que corresponderá aos últimos 60 (sessenta) dias de vigência do contrato:

a) Entrega de Versões Finais de Produtos e Documentação:

- Ao final do contrato, a CONTRATADA deverá entregar ao STM uma cópia final, completa e atualizada de todos os ativos lógicos e documentais produzidos e utilizados durante a prestação do serviço. Isso inclui, no mínimo:
  - Backups de Configuração: Cópia completa das configurações de todos os equipamentos (NGFW e Gerência Centralizada), incluindo políticas de firewall, regras de NAT, configurações de VPN, objetos de rede, políticas de IPS e SD-WAN.
  - Documentação Técnica: Versão final de toda a documentação técnica do ambiente, como diagramas de rede, topologia da solução, manuais de procedimentos específicos e o histórico de mudanças relevantes.

b) Transferência Final de Conhecimentos:

- A CONTRATADA deverá colaborar integralmente em um processo de transição e transferência de conhecimento para a nova equipe que assumirá o serviço (seja de um novo fornecedor ou a equipe interna do STM). Essa colaboração deverá incluir:
  - Reuniões Técnicas: Realização de reuniões para explicar a arquitetura da solução, a lógica por trás das principais políticas de segurança implementadas e quaisquer customizações realizadas.
  - Suporte na Transição: O profissional sênior dedicado deverá estar disponível para sanar dúvidas da nova equipe e acompanhar as fases iniciais da operação assistida pelo novo fornecedor, garantindo uma passagem de bastão suave e sem perda de conhecimento.

c) Devolução de Recursos Materiais:

Sendo um contrato de serviço no qual os equipamentos de hardware não são ativos do STM, a CONTRATADA será a única responsável pela logística de desinstalação e remoção de todos os seus equipamentos físicos das 17 localidades da JMU ao término do contrato. Este processo deverá ser agendado e realizado em coordenação com a equipe da COTEC, sem causar danos à infraestrutura de racks, elétrica ou de cabeamento do STM.

d) Revogação de Perfis de Acesso:

- Este é um procedimento de segurança mandatório. No último dia de vigência do contrato, todos os perfis de acesso, lógicos e físicos, concedidos à equipe da CONTRATADA deverão ser revogados. Isso inclui, mas não se limita a:
  - Acessos de administrador às consoles de gerenciamento dos equipamentos de segurança.
  - Contas de acesso à rede interna do STM.
  - Acessos via VPN.
  - Crachás ou quaisquer outras formas de acesso físico às dependências do STM.
- Este processo deverá ser formalmente executado e auditado pela equipe de segurança da informação do STM.

e) Eliminação de Caixas Postais e Contas de Serviço:

- Quaisquer contas de e-mail, grupos de distribuição ou contas de serviço que tenham sido criadas nos sistemas do STM especificamente para a comunicação ou operação deste contrato deverão ser desativadas ao seu término.

2.5. Estratégia de Independência Tecnológica

O objetivo desta estratégia é garantir que, ao final do contrato de 60 meses, o Superior Tribunal Militar (STM) não se torne refém da tecnologia ou do fornecedor contratado, mantendo a flexibilidade e a autonomia para evoluir sua infraestrutura de segurança da forma que julgar mais vantajosa para a instituição. Para mitigar o risco de "aprisionamento tecnológico" (*vendor lock-in*), serão adotados os seguintes critérios:

2.5.1. Propriedade dos Dados de Configuração e Logs:

Fica estabelecido que todos os dados gerados pela operação da solução, incluindo, mas não se limitando a, logs de eventos, relatórios de segurança, dados de performance e, crucialmente, toda a base de dados de configuração da solução (políticas de firewall, regras, objetos, etc.), são de propriedade exclusiva e inalienável do STM. A CONTRATADA deverá garantir mecanismos para a exportação e entrega desses dados em formato legível e documentado ao final do contrato, conforme estipulado na seção 2.4.

2.5.2. Transferência de Conhecimento e Capacitação Contínua:

A independência tecnológica é construída sobre o conhecimento. As exigências de treinamento para a equipe interna do STM (item 2.2) e a transferência final de conhecimento (item 2.4.b) são pilares desta estratégia. O objetivo é assegurar que a equipe do STM possua o conhecimento necessário para compreender a arquitetura, auditar o serviço e gerenciar uma transição para um novo fornecedor com o mínimo de atrito e perda de informação.

2.5.3. Adoção de Padrões de Mercado:

A solução a ser contratada deve, obrigatoriamente, ser baseada em padrões de mercado abertos e amplamente adotados pela indústria de TIC, como os protocolos IPsec e SSL/TLS para VPN, BGP e OSPF para roteamento, e SAML 2.0 para autenticação. A utilização de protocolos proprietários que criem barreiras para a interoperabilidade com soluções de outros fabricantes será evitada, garantindo que o STM possa integrar a solução de segurança com outras ferramentas e, futuramente, migrar para outras plataformas com maior facilidade.

2.5.4. Direitos sobre a Propriedade Intelectual:

O software embarcado nos equipamentos e o sistema operacional do firewall são de propriedade intelectual do fabricante, e o STM adquire o direito de uso por meio das licenças (subscrições). Contudo, qualquer produto de trabalho intelectual desenvolvido especificamente para o STM no decorrer do contrato — como scripts de automação, modelos de relatórios customizados ou documentação técnica específica — deverá ter seus direitos de uso e modificação perpetuamente cedidos ao STM, sem custos adicionais, garantindo que o conhecimento customizado para o ambiente da JMU seja retido pela instituição.

3. CAPÍTULO 3: ESTRATÉGIA PARA A CONTRATAÇÃO

3.1. Natureza do Objeto

A correta caracterização da natureza do objeto é fundamental para definir o enquadramento orçamentário, o regime de execução e os direitos e deveres das partes.

3.1.1. Classificação da Despesa (Despesa Corrente):

O objeto desta contratação é a prestação de um serviço, e não a aquisição de um bem ou ativo permanente para o Superior Tribunal Militar. A solução, que engloba equipamentos, licenças e serviços profissionais, será fornecida pela CONTRATADA por um período determinado de 60 meses, mediante pagamento de uma mensalidade recorrente. Os equipamentos físicos não serão incorporados ao patrimônio do STM e deverão ser removidos pela CONTRATADA ao final do contrato.

Justificativa: Por se tratar de uma contratação de serviço, a despesa se classifica como Despesa Corrente (Custeio), conforme o elemento de despesa 3.3.90.40 (Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica). Este modelo é vantajoso por proporcionar previsibilidade orçamentária e evitar um grande desembolso de capital para a aquisição de ativos que possuem rápida obsolescência tecnológica.

3.1.2. Natureza do Serviço (Serviço de Natureza Continuada):

O serviço de proteção de perímetro, monitoramento e resposta a incidentes de segurança é caracterizado como de natureza continuada.

Justificativa: A necessidade de proteger os sistemas e as informações da Justiça Militar da União é permanente, essencial e indispensável ao funcionamento diário da instituição. Conforme demonstrado no item 2.3, a interrupção deste serviço resultaria na paralisação das atividades jurisdicionais e administrativas, com prejuízo grave ao interesse público. A natureza contínua justifica a possibilidade de um contrato com vigência estendida de 60 meses, garantindo a estabilidade e a maturidade da solução e do serviço prestado.

3.1.3. Direitos de Propriedade Intelectual:

A definição dos direitos de propriedade intelectual é crucial para garantir a autonomia e a independência tecnológica do STM, conforme a estratégia delineada no item 2.5. A propriedade intelectual é dividida da seguinte forma:

- **Solução Base (Hardware e Software):** A propriedade intelectual do software embarcado nos equipamentos (sistema operacional do firewall) e do design do hardware pertence exclusivamente ao **fabricante** da tecnologia. O STM e a CONTRATADA adquirem o direito de uso dessa tecnologia por meio das licenças (subscrições) durante a vigência do contrato.
- **Artefatos e Configurações Produzidos para o STM:** A propriedade intelectual de todos os dados, configurações, relatórios customizados, documentação técnica, diagramas e quaisquer outros artefatos que sejam produzidos e customizados **especificamente para o ambiente do STM** durante a execução do contrato **pertencerá integralmente ao Superior Tribunal Militar (STM)**.

Justificativa: Essa distinção é fundamental. Enquanto o STM não pode ser dono do produto principal do fabricante, é imperativo que seja dono de toda a "inteligência" e customização aplicadas ao seu ambiente. A posse dos dados de configuração, por exemplo, é o que garante que o STM possa, ao final do contrato, migrar para um novo fornecedor ou plataforma sem perder todo o trabalho de desenvolvimento de políticas de segurança, assegurando sua independência tecnológica.

3.2. Parcelamento do Objeto e Adjudicação

3.2.1. Justificativa do Não Parcelamento do Objeto:

a) A regra geral na administração pública é o parcelamento do objeto, visando ampliar a competitividade. No entanto, para a presente contratação, o parcelamento se mostra tecnicamente inviável e antieconômico, representando um risco inaceitável para a segurança e a operação do STM.

b) O objeto contratual não é uma soma de partes independentes, mas sim um serviço único e indivisível de Segurança Gerenciada. A eficácia da solução depende da sinergia total entre o hardware (NGFW), o software (licenças de segurança), o serviço de monitoramento (SOC/NOC) e o suporte especializado (profissional dedicado).

c) A tentativa de parcelar este objeto — por exemplo, licitando os equipamentos com uma empresa e o serviço de gerenciamento com outra — resultaria em graves prejuízos técnicos e de gestão, tais como:

- **Diluição de Responsabilidade:** Em caso de falha ou incidente de segurança, haveria um conflito para determinar a responsabilidade. O fornecedor do equipamento poderia culpar a má configuração feita pela empresa de serviços, e vice-versa, deixando o STM como árbitro de uma disputa técnica complexa em um momento de crise.
- **Complexidade de Gestão Contratual:** O STM teria que gerenciar dois ou mais contratos distintos para uma única finalidade, duplicando o esforço de fiscalização e a sobrecarga administrativa.
- **Inviabilidade de Aplicação do SLA:** Seria impraticável responsabilizar uma das partes pelo não cumprimento do Acordo de Nível de Serviço, pois a causa raiz de um problema de performance ou disponibilidade poderia ser atribuída à outra parte do serviço parcelado.

Conclui-se, portanto, que a natureza integrada do serviço exige um fornecedor único que seja totalmente responsável pela solução de ponta a ponta. A contratação do objeto em um item único é a única forma de garantir a responsabilidade, a coesão técnica e a eficácia do serviço de segurança.

3.2.1. Adjudicação do Objeto

a) Diante da indivisibilidade do objeto, a licitação terá como critério de adjudicação o menor preço global para o item único, que engloba todos os equipamentos, licenças e serviços descritos para o período de 60 meses.

b) Permissão de Consórcio e Subcontratação:

Consórcio: Será permitida a participação de empresas em consórcio, como forma de ampliar a competitividade e permitir a união de expertises, desde que atendidas todas as exigências de qualificação técnica e habilitação jurídica e fiscal previstas no edital.

Subcontratação: Será permitida a subcontratação de partes do serviço, como, por exemplo, o monitoramento de primeiro nível pelo SOC/NOC. No entanto, a permissão estará sujeita às seguintes condições estritas:

- A empresa CONTRATADA permanecerá como a única e total responsável perante o STM por todas as obrigações contratuais, incluindo o cumprimento integral do SLA.
- Será expressamente vedada a subcontratação do profissional sênior dedicado. Este recurso é considerado o núcleo da expertise e do relacionamento técnico com o STM e deve ser um funcionário direto da CONTRATADA.
- A subcontratação deverá ser previamente aprovada pelo STM.

3.3. Modalidade e Tipo de Licitação

3.3.1. Modalidade de Licitação: Pregão, na sua forma Eletrônica.

Justificativa: O objeto da contratação, embora tecnicamente complexo, enquadra-se na definição de serviço comum, nos termos da Lei nº 14.133/2021. Seus padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado, conforme detalhado exaustivamente neste Estudo Técnico Preliminar e será consolidado no Termo de Referência. A existência de um mercado competitivo, com múltiplos fornecedores capazes de atender aos requisitos, reforça essa caracterização. Conforme a legislação vigente, a utilização da modalidade Pregão é obrigatória para a contratação de bens e serviços comuns, sendo a sua forma eletrônica a preferencial por ampliar a competitividade e a transparência do certame.

3.3.2. Tipo de Licitação (Critério de Julgamento): Menor Preço.

Justificativa: Uma vez que todas as especificações técnicas, níveis de serviço (SLA) e requisitos de qualificação da CONTRATADA e de seus profissionais serão definidos de forma clara e objetiva no Termo de Referência como critérios mínimos e obrigatórios para participação, a qualidade da solução estará assegurada para todas as propostas válidas. Dessa forma, o critério que melhor atenderá ao interesse público será o de Menor Preço Global para o item único, garantindo que o STM contratará o serviço que atende a todos os requisitos de qualidade necessários com o menor dispêndio de recursos.

3.3.3. Adoção do Sistema de Registro de Preços (SRP):

A licitação será processada por meio do **Sistema de Registro de Preços (SRP)**, resultando em uma Ata de Registro de Preços com validade de 12 (doze) meses, a partir da qual será firmado o contrato de prestação de serviço.

Justificativa: A adoção do SRP é a estratégia mais vantajosa para esta contratação devido à necessidade de uma implementação em fases, que otimiza a logística e o planejamento da equipe técnica. A execução do projeto seguirá uma ordem de prioridade:

a) Fase 1 (Implementação Imediata): Após a assinatura da Ata, será emitida a primeira Ordem de Serviço para a implantação da infraestrutura crítica no Data Center da Sede do STM. Isso inclui os 2 (dois) equipamentos do Tipo I em alta disponibilidade e o Serviço de Gerência Centralizada. Esta fase estabelece o núcleo da nova solução de segurança.

b) Fases Subsequentes (Implementação Sob Demanda): A implantação dos equipamentos nas 16 (dezesseis) Auditorias remotas (Tipos II, III e IV) ocorrerá de forma planejada e faseada ao longo da vigência da Ata.

Esta abordagem proporciona ao STM a flexibilidade necessária para coordenar a complexa logística de instalação em múltiplas unidades federativas, permitindo o agendamento de janelas de manutenção e a alocação de equipes de forma mais eficiente. Além disso, o SRP garante os preços e o fornecedor para toda a solução desde o início, mas permite que os desembolsos orçamentários acompanhem o cronograma de implantação física, em alinhamento com os princípios da eficiência e do planejamento administrativo.

3.4. Vigência do contrato

a) Prazo de Vigência: O prazo de vigência do contrato para a prestação do Serviço Gerenciado de Segurança da Informação será de 60 (sessenta) meses, contados a partir da data de sua assinatura, podendo ser renovado na forma da lei.

b) Relação com a Ata de Registro de Preços (SRP): Conforme definido no item 3.3, a licitação será realizada por meio do Sistema de Registro de Preços. A Ata de Registro de Preços resultante terá validade de 12 (doze) meses, podendo ser renovada na forma da lei. O contrato de 60 meses será assinado com base nesta Ata, e as Ordens de Serviço para a implantação dos equipamentos nas diversas localidades da JMU serão emitidas durante a vigência da Ata.

b) Justificativa para o Prazo de 60 meses:

- Natureza do Serviço e Amparo Legal: O objeto foi classificado como serviço de natureza continuada. A Lei nº 14.133/2021 permite que contratos desta natureza tenham duração inicial de até 5 (cinco) anos (60 meses), conferindo amparo legal para o prazo estipulado.
- Viabilidade Econômica: A contratação envolve um investimento inicial significativo por parte da CONTRATADA no fornecimento de 18 equipamentos de hardware de alto valor. Um prazo de vigência de 60 meses permite a amortização desse investimento ao longo do tempo, resultando em um valor de mensalidade consideravelmente menor para o STM. Um prazo mais curto tornaria o valor mensal do serviço proibitivo.
- Estabilidade e Maturidade do Serviço: Um contrato de longo prazo é fundamental para a maturação do serviço prestado. Ele permite que a equipe da CONTRATADA e, em especial, o profissional dedicado, desenvolvam um profundo conhecimento sobre o ambiente, a cultura e as necessidades específicas do STM, resultando em um serviço mais estável e proativo.
- Redução de Custos Administrativos: A celebração de um contrato de 60 meses evita a necessidade de realizar novos e complexos processos licitatórios a cada 12 ou 24 meses, reduzindo significativamente a carga de trabalho das áreas administrativa e técnica do STM.

c) Da Possibilidade de Prorrogação Contratual:

Além do prazo inicial de 60 meses, o contrato poderá ser prorrogado por sucessivos períodos, conforme previsto para serviços de natureza contínua na Lei nº 14.133/2021, observado o limite máximo de 10 (dez) anos de duração total.

Justificativa: A Lei nº 14.133/2021 prevê esta possibilidade, desde que haja previsão no edital e que a vantajosidade econômica da prorrogação para a Administração seja demonstrada a cada termo aditivo. A inclusão desta previsão no edital é estratégica, pois, caso a prestação do serviço se mostre excelente e os preços se mantenham competitivos frente ao mercado, a prorrogação do contrato é a medida de maior eficiência administrativa. Ela evita os custos, os riscos e a descontinuidade operacional inerentes a um novo processo licitatório e a uma nova migração de serviço, preservando a estabilidade e o conhecimento adquirido sobre o ambiente do STM.

3.5. Equipe de Apoio à Contratação

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).

A indicação do Integrante Administrativo consta do Documento de Oficialização da Demanda – DOD 4235747

A Equipe de Planejamento da Contratação foi instituída pelo Senhor Diretor-Geral - Portaria 10161 (4241916)

3.6. Equipe de Gestão do Contrato

A Equipe de Gestão do Contrato desta contratação será composta pelos servidores Wilson Marques de Souza Filho (Gestor), Márcio Coelho Marques (Integrante Demandante), Claudio de Oliveira Melo (Integrante Técnico) e Luis Gustavo Costa Reis (Integrante Administrativo).

5 – APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pela Portaria 10164 (4241916).

Conforme a Resolução Nº 468 de 15 de julho de 2022 do CNJ o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Demandantes e pela autoridade máxima da área de TIC:

INTEGRANTE DEMANDANTE	INTEGRANTE TÉCNICO	INTEGRANTE ADMINISTRATIVO
WILSON MARQUES DE SOUZA FILHO Coordenador	**MARCIO COELHO MARQUES** Chefe de Seção	**LUIS GUSTAVO COSTA REIS** Analista Judiciário

AUTORIDADE MÁXIMA DA ÁREA DE TIC

IANNE CARVALHO BARROS
Diretor de Tecnologia da Informação

Documento assinado eletronicamente por **WILSON MARQUES DE SOUZA FILHO**, **COORDENADOR DE INFRAESTRUTURA DE TECNOLOGIA**, em 14/10/2025, às 18:09 (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 15/10/2025, às 13:58 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCIO COELHO MARQUES**, **ANALISTA JUDICIÁRIO - Apoio Especializado - Análise de Sistemas**, em 15/10/2025, às 14:24 (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 E TRANSFORMAÇÃO DIGITAL**, em 15/10/2025, às 15:18 (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 **4510789** e o código CRC **1DA059E6**.