



SUPERIOR TRIBUNAL DE JUSTIÇA
SAFS - Quadra 6 - Lote 1 - Trecho III - CEP 70095-900 - Brasília - DF - www.stj.jus.br

ESTUDOS TÉCNICOS PRELIMINARES
SERVIÇOS DE TIC SEM MÃO DE OBRA

1. Informações Gerais
1.1 N. do Processo SEI: 043526/2022
1.2 Unidade Requisitante: CSID - Coordenadoria de Segurança da Informação e Defesa Cibernética
1.3 Unidade Técnica: SESEG - Seção de Segurança da Informação
1.4 Houve uma centralização da solicitação de diversas unidades? (x) Não se aplica () A unidade centralizou as solicitações das seguintes unidades: _____
1.5 Equipe de planejamento da contratação ou servidor responsável: 1.5.1 - Integrantes Requisitantes Nome: Edimar Lisboa das Chagas - Unidade: CSID - Coordenadoria de Segurança da Informação e Defesa Cibernética (Titular) Nome : Luciano Viana de Oliveira - Unidade: SERIT - Seção de Conformidade e Riscos de TIC (suplente) 1.5.2 - Integrantes Técnicos Nome: Vitor Gabriel Jaime Paiva - Unidade: SESEG - Seção de Segurança da Informação (Titular) Nome: Uriel Kádmo Nunes Torres - Unidade: SEGAE - Seção de Gestão de Acesso e Eventos de Segurança (Suplente) 1.5.3 - Integrantes Administrativos Nome: Winston Luiz de Oliveira Rodrigues - Unidade: SMTIC - Seção de Monitoramento e Planejamento de Contratos de TIC (Titular) Nome: Jessica Souto Ferreira - Unidade: SMTIC - Seção de Monitoramento e Planejamento de Contratos de TIC (Suplente)
1.6 Responsável pela aprovação do Estudo Preliminar: Nome: Humberto Fontoura Pradera Secretaria/Assessoria: STI - Secretaria de Tecnologia da Informação e Comunicação
1.7 Fiscais e gestores: Fiscal Técnico: Nome: Vitor Gabriel Jaime Paiva - Unidade: SESEG - Seção de Segurança da Informação (Titular) Nome: Uriel Kádmo Nunes Torres - Unidade: SEGAE - Seção de Gestão de Acesso e Eventos de Segurança (Suplente) Fiscal Requisitante: Nome: Edimar Lisboa das Chagas - Unidade: CSID - Coordenadoria de Segurança da Informação e Defesa Cibernética (Titular) Nome : Luciano Viana de Oliveira - Unidade: SERIT - Seção de Conformidade e Riscos de TIC (suplente) Fiscal Administrativo: A indicação será definida pelo Titular da SMTIC - Seção de Monitoramento e Planejamento de Contratos de TIC. Gestor: A indicação será definida pelo Titular da SCONT - Seção de Gestão de Contratações de TIC Comissão de Recebimento: A indicação será definida pelo Titular da CSID - Coordenadoria de Segurança da Informação e Defesa Cibernética.
2. Necessidade da contratação
2.1 Descrição da Necessidade: Solução de microssegmentação A microssegmentação é uma técnica de segurança de rede que permite aos arquitetos de segurança dividir logicamente o data center em segmentos de segurança distintos até o nível de carga de trabalho individual e, em seguida, definir controles de segurança e fornecer serviços para cada segmento separadamente. A microssegmentação permite que TI implante políticas de segurança flexíveis profundamente aninhadas em um data center por meio da tecnologia de virtualização de redes, em vez de instalar vários firewalls físicos. Além disso, a microssegmentação pode ser usada para proteger cada máquina virtual (VM, pela sigla em inglês) em uma rede corporativa com controles de segurança no nível do aplicativo e orientados por políticas. Como as políticas de segurança são aplicadas a cargas de trabalho separadas, o software de microssegmentação pode aumentar significativamente a resistência de uma empresa contra ataques. A microssegmentação se baseia na tecnologia de virtualização em nível de rede, criando zonas seguras e estritamente adequadas às necessidades de comunicação entre os ativos de rede, independentemente de segmentação na camada 3, possibilitando abordagens detalhadas e específicas. A microssegmentação acarreta em uma melhora na segurança da rede e também impacta em melhoria no desempenho, otimizando o tráfego e reduzindo congestionamentos. O Gartner (https://www.gartner.com/reviews/market/microsegmentation, acessado em 26 de Outubro de 2023) define a microssegmentação como a capacidade de inserir uma política de segurança na camada de acesso entre duas cargas de trabalho, dentro do mesmo data center estendido. As tecnologias de microssegmentação possibilitam a definição de zonas de rede altamente granulares, chegando até ativos e aplicativos individuais. As capacidades principais incluem: • Mapeamento de fluxo, que é a capacidade de coletar e mostrar fluxos de tráfego Norte/Sul e Leste/Oeste e utilizá-los na definição de políticas (podendo apresentar esses dados visualmente). • Isolamento de cargas de trabalho, que consiste no isolamento em relação a outras cargas de trabalho com base em políticas de segurança. • Aplicação de políticas, incluindo a definição de regras com base em diferentes fatores. • A capacidade de implantação em ambientes virtualizados e de infraestrutura como serviço. A Gartner afirma ainda que até 2026, 60 por cento das corporações que objetivam uma arquitetura "zero trust" estarão utilizando soluções de microssegmentação. No ano de 2023, porém, esse número está por volta de 5 por cento (Gartner Market Guide for Microsegmentation, publicado em 12 de Junho de 2023 - SEI 3790056). A Forrester também corrobora com a importância da microssegmentação, afirmando no <i>New Wave</i> de 2022 que "<i>A microssegmentação é essencial para redes privadas de zero trust</i>".
2.2. Problema a ser resolvido Solução de microssegmentação

Em virtude do comportamento padrão das redes de computadores, o tráfego de rede entre dispositivos localizados no mesmo segmento não passa por nenhuma camada de segurança, ocorrendo diretamente entre os dispositivos. Esse comportamento dificulta na identificação e monitoramento dentro do segmento, o que pode resultar em uma vulnerabilidade inerente ao chamado tráfego "leste-oeste".

Para contornar essa situação, a tecnologia de microssegmentação atua diretamente na interface de rede dos ativos, viabilizando a implantação de políticas de firewall, IPS, *antimalware* diretamente na placa de rede, ou seja, ela pode bloquear atividades maliciosas que estejam ocorrendo dentro de um único segmento de rede. Desta forma, mesmo que existam dispositivos desconhecidos ou incorretamente conectados em determinado segmento da rede, esses ativos não conseguirão se comunicar com as máquinas de produção do Tribunal, uma vez que todo o tráfego desconhecido será sumariamente descartado pela solução de microssegmentação da rede.

A microssegmentação é uma estratégia avançada de segurança de redes que resolve problemas de segurança e desempenho do próprio protocolo TCP/IP. É possível fazer um controle no nível mais granular da comunicação, chegando em algumas situações até no nível de processo que pode efetuar uma comunicação, e bloqueando qualquer outro tipo de comunicação daquele dispositivo.

Além disso, com a implementação de uma solução de microssegmentação se consegue melhorar a performance da rede, uma vez que reduz a quantidade de pacotes broadcast no segmento e consequentemente reduzindo congestionamentos.

Com a microssegmentação de redes, é possível reduzir a superfície de ataque do ambiente, evitar a movimentação lateral e reduzir sensivelmente o risco de segurança nos dispositivos de TIC.

A granularidade adicional implícita na microssegmentação permite a implementação de políticas de segurança por meio de virtualização de rede. Desta forma, as máquinas virtuais e servidores ficam isolados e protegidos, inclusive de ataques internos que possam ocorrer. É uma forma inclusiva de se proteger dos ataques "insider", ou seja, quando a ameaça cibernética se encontra dentro da própria organização. Insiders podem causar danos muito mais graves do que hackers externos podem, porque eles têm acesso muito mais fácil à sistemas e uma janela maior para suas atividades ilícitas. Os danos causados por atacantes internos podem incluir a suspensão das operações, perda de propriedade intelectual, danos à reputação da empresa, perda de investidores e confiança do cliente, vazamentos de informações confidenciais para terceiros, incluindo os meios de comunicação. De acordo com várias estimativas, pelo menos 80 milhões de ataques internos ocorrem nos Estados Unidos todos os anos. Mas o número pode ser muito maior, porque muitas vezes eles não são declarados. Claramente, o seu impacto totaliza agora na casa das dezenas de bilhões de dólares por ano.

3. Requisitos da contratação

3.1 Requisitos de Negócio

- Solução estável e madura, com histórico de sucesso no mercado;
- Alta disponibilidade e tolerante à falhas;
- Não deve possuir pontos únicos de falha;
- Capaz de se recuperar da queda de um datacenter em poucos segundos;
- Desempenho superior ao atual;
- Capaz de atender ao crescimento dos próximos cinco anos;
- Que utilize uma infraestrutura padrão de mercado (hardware e sistema operacional);
- Simplifique a gestão da infraestrutura, reduzindo a complexidade e a quantidade de contratos;
- Possua suporte especializado com o fabricante do hardware e do software;
- Conter todo o hardware e software necessário para o correto funcionamento da solução;
- Licenciar todas as funcionalidades;
- Não deve impactar nos serviços prestados pela Corte;
- Deve aumentar o nível de segurança no datacenter;
- Deve ter uma gerência centralizada;
- Não deve onerar os servidores do ambiente;
- Deve ser o mais transparente possível;
- O licenciamento deve ser flexível e não limitado ao tipo de ativo;
- O licenciamento de microssegmentação deverá compreender todo o ambiente de datacenter do Superior Tribunal de Justiça;

3.2 Requisitos de Capacitação e Treinamento

- A empresa deverá comprovar, 10 dias após a assinatura do Contrato, que dispõe de um quadro de técnicos certificados, que, obrigatoriamente deverá abranger, de forma coletiva, a certificação emitida pelo fabricante da solução.
- A Contratada deverá ministrar transferência de conhecimento e disponibilizar o material didático, oficial do fabricante, devendo abordar no mínimo os seguintes itens:
 - Transferência de conhecimento (*hands-on e mentoring*);
 - Visão geral dos recursos e funcionalidades da solução;
 - Overview e considerações sobre a arquitetura do produto;
 - Tarefas básicas de administração, monitoração e manutenção;
 - Planejamento de recursos para instalação;
 - Instalação, configuração e administração;
 - Todos os procedimentos necessários à instalação física e lógica; configuração técnica, e à completa operação dos produtos;
 - Gerenciamento de recursos;
 - Configuração de dispositivos;
 - Gerenciamento de planos de recuperação de dados;
 - Criação de políticas;
 - Troubleshooting e resolução de problemas comuns;
 - Todos os procedimentos de manutenção dos produtos;
 - Cobre adequadamente os conhecimentos necessários para administração, configuração, otimização, troubleshooting e utilização da solução;
 - Foco na implementação e manutenção do ambiente de produção;
 - Planejamento e implementação de projeto de *disaster recovery* utilizando a ferramenta;
 - Planejamento de capacidade;
 - Análise de riscos;
 - Deverá ser ministrado por profissional certificado pelo fabricante do produto ofertado, em Brasília;
 - Toda a logística é responsabilidade da CONTRATADA;
 - Realizar laboratórios práticos entre cada unidade de conhecimento;
 - Será realizado em dias úteis, sempre iniciando na segunda-feira, salvo se expresso em contrário pelo STJ;
 - Disponibilizar, para todos os participantes, material oficial do fabricante, atualizado e de primeiro uso, em português ou inglês;
- A critério do STJ, pode ser admitida a modalidade *online*, não eximindo a CONTRATADA de atender todos os requisitos listados anteriormente.

3.3 Requisitos de Manutenção

- A Contratada é responsável pelo suporte e garantia dos equipamentos/softwarees fornecidos;
- Atendimento 24x7 nas dependências do STJ;
- Deve fornecer opções de suporte técnico preferencialmente no idioma português do Brasil;
- Prestar serviços de assistência técnica à solução, abrangendo manutenção preventiva programada, manutenção corretiva e suporte técnico com fornecimento de peças;
- Atualizar e evoluir os softwares e firmwares nativos da solução, em termos de versionamento, releases, fixes e aplicativos de correção;
- Substituir componentes e peças defeituosos ou com falhas, trocas periódicas das peças internas, discos e demais componentes que apresentarem problemas técnicos durante a vigência do contrato, utilizando de produtos originais, novos e de primeiro uso, garantidos pelo fabricante;
- Elaborar cronograma de análises e manutenções preventivas, em dias úteis, para cada subsistema ou área do objeto contratado, possibilitando à equipe técnica a adequação necessária para implantação e execução dos serviços;
- Prestar os serviços dentro dos parâmetros e rotinas estabelecidos no processo de contratação, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios;
- Possibilitar o suporte técnico e especializado, remoto ou presencial, entre o CONTRATANTE e o fabricante sem novos ônus ou custos contratuais;
- Executar todas as atividades de instalação, atualização, configuração e migração de acordo com o planejamento aprovado pela área técnica;
- Realizar manutenção preventiva programada, que se destina a prevenir indisponibilidades e/ou falhas dos componentes da solução contratada, em suas instalações, subsistemas e componentes envolvidos, mantendo-as em perfeito estado de funcionamento e conservação, conforme especificado em projeto, manuais e normas técnicas específicas;
- Realizar manutenção corretiva, que compreende providências para reparar e corrigir os componentes da solução contratada em seu pleno estado de funcionamento, removendo definitivamente os defeitos eventualmente apresentados;
- Realizar a manutenção evolutiva dos hardwares e softwares da solução, fornecendo, instalando e configurando as novas versões, *releases* e atualizações lançadas durante a vigência contratual, mantendo-os funcionais e compatíveis com o ambiente utilizado pelo STJ;
- Garantir o funcionamento do ambiente com relação à solução instalada pela CONTRATADA, incluindo todos os serviços necessários para manutenção da disponibilidade da solução, inclusive de configurações e fornecimento de "firmwares", "fixes" e "releases", durante toda a vigência do contrato;
- O atendimento para requisições de suporte deve ocorrer em regime 24x7.

3.4 Requisitos de Conformidade

- Deverá fazer parte do catálogo de produtos comercializados pelo fabricante e não ter sido descontinuado;
- Deverá ser novo, sem uso, e constar no site do fabricante (documento oficial e público) como em linha de produção;
- Deverá ser entregue na versão mais recente conforme indicado pelo fabricante;
- Deverá ser totalmente compatível com o ambiente de datacenter do STJ, a saber, VMware vSphere, vCenter e vSAN versão 8.x;
- Deverá permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, durante a vigência contratada, irrestrita e sem necessidade de licenciamentos ou ônus adicionais.

3.5 Requisitos Temporais

- Apresentar plano de implantação contendo os requisitos de instalação e cronograma de entrega, instalação, configuração e disponibilização da solução, em até 30 (trinta) dias corridos da assinatura do contrato;
- Entregar os produtos no prazo máximo de até 30 (trinta) dias corridos, a contar da assinatura do contrato,
 - A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE;
 - Executar a conferência dos produtos especificados, conjuntamente com representantes da CONTRATADA, para emissão do Termo de Recebimento Provisório;
 - Antes de findar o prazo fixado a empresa CONTRATADA poderá formalizar, de forma devidamente fundamentada, pedido de sua prorrogação, cujas razões expostas serão examinadas pela administração do CONTRATANTE, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas;

- A CONTRATADA receberá cópia do “Termo de Recebimento Provisório” após a entrega e conferência dos produtos em até 5 (cinco) dias úteis da confirmação de entrega, contados do primeiro dia imediatamente posterior à confirmação de entrega dos itens no CONTRATANTE, desde que não haja pendências de responsabilidade da CONTRATADA;
- Concluir, no prazo de 90 (noventa) dias corridos, a contar da emissão do termo de recebimento provisório, a implantação e configuração dos produtos, em plena compatibilidade com o ambiente computacional do CONTRATANTE e em conformidade com a proposta técnica apresentada, cumprindo ainda todas as demais cláusulas de garantia e atendimento técnico constantes do contrato, nos prazos e termos ali estipulados;
- A CONTRATADA receberá cópia do “Termo de Recebimento Definitivo”, que deverá ser providenciado pelo CONTRATANTE no prazo máximo de 10 (dez) dias úteis, após manifestação da CONTRATADA de conclusão dos serviços e comprovação de atendimento de todas as fases, desde que a CONTRATADA atenda a todas as solicitações e que não haja pendências de sua responsabilidade;
- Os serviços de suporte e garantia deverão estar disponíveis para atendimento durante os 07 (sete) dias corridos da semana, 24 (vinte e quatro) horas por dia;
- Considerar o horário de 07:00 horas às 21:00 horas como de horário normal de expediente, para os dias úteis;
- Deverá ser gerado relatório mensal de todas as atividades realizadas nas visitas técnicas e manutenções dos equipamentos.

3.6 Requisitos de Segurança da Informação

- Garantir a confidencialidade, mesmo após o término do prazo de vigência ou rescisão do contrato, das informações relativas:
 - À política de segurança adotada;
 - Ao processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos;
 - Ao processo de implementação, no ambiente do CONTRATANTE, dos mecanismos de criptografia e autenticação;
- Respeitar os critérios, padrões, normas e procedimentos operacionais adotados pelo CONTRATANTE;
- Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste contrato, devendo orientar seus empregados nesse sentido;
- Promover condições de entendimento das normas de acesso à instituição, tratamento pessoal, comportamento e trânsito, assim como as soluções utilizadas caso infringidas;
- A solução deve ser dimensionada e configurada para suportar a perda de qualquer componente sem impacto para o serviço;
- Atender às melhores práticas do CIS Control;
- Deverá isolar o tráfego leste-oeste, independente da configuração em camada 3;
- Deverá possibilitar a aplicação de patches de segurança "virtuais" para proteger ativos que porventura tenham alguma limitação de atualização.

3.7 Requisitos Sociais, Ambientais e Culturais

- Deverá declarar ter conhecimento da Política de Sustentabilidade do CONTRATANTE, dando cumprimento aos dispositivos da [Instrução Normativa STJ/GDG nº 15, de 12 de novembro de 2020](#), que instituiu a Política de Sustentabilidade no STJ e os profissionais a serem designados para o trabalho local deverão estar informados sobre as boas práticas voltadas ao consumo consciente, redução de desperdício dos recursos naturais e coleta seletiva;
- O preposto ou representante técnico, quando atuar no STJ, deverá responsabilizar-se pela limpeza e conservação dos ambientes onde desempenhe seus serviços;
- Deverá, inclusive, encaminhar adequadamente os resíduos porventura gerados na execução do contrato, com o objetivo de contribuir para a preservação do meio ambiente;
- Os profissionais destacados para prestação de serviços no STJ deverão estar informados sobre as boas práticas voltadas ao consumo consciente, redução de desperdício e coleta seletiva, com o objetivo de contribuir para a preservação do meio ambiente e dos recursos públicos.

3.8 Requisitos de arquitetura tecnológica

- A solução fornecida e os serviços prestados deverão se adequar aos elementos da arquitetura tecnológica existente, mantendo-a operacional durante a vigência contratual, nas mesmas condições funcionais e de disponibilidade do período de início de execução do contrato;
- Deverá garantir a alta disponibilidade para a solução de microssegmentação nos datacenters;
- Suportar arquitetura de alta disponibilidade HA (*High Availability*);
- A solução deve ser fornecida com todos os acessórios necessários para a plena configuração, operacionalização, utilização e gerenciamento do equipamento, sem necessidade de aquisições futuras de licenças ou softwares de ativação, tais como:
 - Softwares e manuais necessários para o gerenciamento;
 - Softwares, drivers e firmwares necessários em suas últimas versões;
- A Console de gerenciamento deverá ser única e centralizada para toda a solução;
- A solução deverá ser totalmente integrada e compatível com o ambiente VMware do Tribunal;
- A solução não deve utilizar agentes instalados nos servidores virtuais, devendo ser o mais transparente e não intrusivo possível;
- A solução deverá ser capaz de ser implantada em vários segmentos de rede, independente do equipamento utilizado para controlar as VLANs;
- A solução deverá possuir a capacidade de etiquetar todos os ativos do datacenter;
- Deve ser possível a concessão de permissões granulares ao ambiente, independente das permissões existentes no ambiente de vCenter.

3.9 Requisitos de projeto e de implementação

- Apresentar o projeto executivo ou de implantação dentro do prazo estipulado contratualmente, que deverá dispor sobre o cronograma de todas as etapas de implantação da solução, previsão de recursos, pessoas envolvidas, requisitos necessários para instalação, atividades a serem desenvolvidas por cada uma das partes, indicação dos principais riscos e forma de mitigação;
- O projeto deverá relacionar e tratar, no mínimo, os seguintes tópicos:
 - Preparação do ambiente de instalação, se for o caso;
 - Instalação e configuração;
 - Teste do HA (disponibilidade e resiliência);
 - Teste de operação;
 - Ativação da solução (aplicação do licenciamento);
 - Entrega da documentação atualizada;
- Elaborar cronograma de instalação e configuração;
- Atividades executadas dentro dos datacenters deverão ocorrer preferencialmente em período fora do expediente, finais de semana e feriados.

3.10 Requisitos de implantação

- Efetuar a atualização dos equipamentos da solução de forma a não impactar as atividades diárias dos usuários;
- Executar fielmente o objeto contratado, de acordo com as normas legais, em conformidade com a proposta apresentada e as orientações do CONTRATANTE, observando sempre os critérios de qualidade;
- Executar o objeto em conformidade com as determinações dos fabricantes, normas técnicas pertinentes, especificações constantes na proposta apresentada e, ainda, de acordo com as definições nas Ordens de Serviços demandadas pelo CONTRATANTE.
- Entregar todos os componentes da solução, hardware software e licenças de ativação necessários à perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração, conforme especificações constantes no Edital;
- Efetuar eventuais adequações ou serviços nos ambientes do CONTRATANTE que se façam necessários para a instalação dos equipamentos e configuração dos softwares, com anuência e autorização prévia do STJ;
- Incluir nos projetos as especificações dos equipamentos, dos cabos e de todos os materiais e equipamentos necessários ao perfeito funcionamento da solução, os quais deverão satisfazer os requisitos mínimos definidos nos processos de padronização do CONTRATANTE;
- Entregar os equipamentos, as licenças de ativação e os respectivos componentes, às suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos cotados;
- Instalar os equipamentos e as licenças de ativação nas datas e horários definidos pela equipe técnica do CONTRATANTE, que supervisionará os trabalhos;
- Realizar todos os trabalhos sem que haja a necessidade de parada do ambiente em produção, exceto as predeterminadas com a equipe do CONTRATANTE. Do mesmo modo, deverão ser observadas as rotinas internas da Organização, cujo andamento em hipótese nenhuma deverá ser prejudicado em razão de quaisquer das atividades a serem contratadas;
- Implantar adequadamente o planejamento, a execução e a supervisão permanente das tarefas demandadas, de forma a obter uma operação correta e eficaz, realizando os serviços de forma metódica e constante, mantendo sempre em perfeita ordem todas as dependências do CONTRATANTE;
- Prestar, de imediato, todos os esclarecimentos solicitados pela fiscalização do CONTRATANTE no que diz respeito ao cumprimento do objeto contratado;
- Permitir acesso exclusivo de técnicos autorizados e em horários previstos de acordo com seus controles e manutenções.

3.11 Requisitos de garantia e manutenção

- A garantia deve ser prestada para todos os itens da solução, conforme as indicações do fabricante;
- Realizar a manutenção evolutiva da solução, fornecendo, instalando e configurando as novas versões, releases e upgrades lançadas durante a vigência contratual, mantendo-os funcionais e compatíveis;
- Disponibilizar número telefônico, com disponibilidade de 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, para fins de abertura de chamados técnicos, assim como para acompanhamento da solução de problemas;
- Disponibilizar os serviços de manutenção durante os 7 (sete) dias da semana, 24 (vinte e quatro) horas por dia, executando-os sempre que aberto um chamado técnico pelo CONTRATANTE;
- Atender ao chamado técnico do CONTRATANTE, para fins de prestação dos serviços de manutenção, encaminhando um técnico até o local onde se encontram instalados os componentes da solução;
- Arcar com as despesas de desinstalação, retirada, deslocamento e reinstalação de componentes a serem mantidos ou substituídos;
- Depois de concluído o chamado ou a manutenção de qualquer equipamento, registrar detalhadamente em relatório próprio todos os procedimentos adotados para a solução dos problemas encontrados, onde constem informações referentes às substituições de peças, identificação do chamado, data e hora do chamado, início e término do atendimento. Tais informações deverão constar dos relatórios mensais;
- Comunicar ao CONTRATANTE por escrito, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os equipamentos e componentes objeto deste contrato, fazendo constar a causa de inadequação e a ação devida para sua correção;
- Assumir a responsabilidade por qualquer acidente de trabalho, danos ou prejuízos causados ao CONTRATANTE e a terceiros;
- Fornecer toda a mão-de-obra qualificada para a execução dos trabalhos;
- Refazer os trabalhos recusados pelo CONTRATANTE;
- Assumir todas as despesas relativas à execução dos serviços, tais como mão-de-obra, ferramentas, equipamentos, taxas, emolumentos e encargos sociais;
- Colocar seu corpo técnico à disposição do CONTRATANTE para orientação quanto à execução dos serviços, sempre que solicitado;
- Não transferir a outrem, no todo ou em parte, o objeto do contrato a ser firmado, sem prévia e expressa anuência do CONTRATANTE;
- Não efetuar, sob nenhum pretexto, a transferência de qualquer responsabilidade da empresa contratadora para outras entidades, sejam fabricantes, técnicos, subempreiteiros etc.;
- Responder por todo e qualquer dano ou prejuízo eventualmente causado ao CONTRATANTE ou a terceiros, como consequência de atos e fatos imputáveis a seus técnicos;
- Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do CONTRATANTE;
- Manter, durante toda a execução dos serviços, as condições de habilitação e qualificação exigidas na licitação;
- Prestar informações técnicas à equipe do CONTRATANTE quanto à operação do ambiente;
- Executar os procedimentos de manutenção e suporte em conformidade com as recomendações dos fabricantes, documentações existentes e as boas práticas de mercado;
- Fornecer avaliação e ajustes para novas instalações no ambiente quando demandados pelo CONTRATANTE;
- Efetuar análise e proposição de soluções adequadas para o ambiente contratado, sob orientação da equipe técnica do CONTRATANTE;
- Fornecer acesso à base de conhecimento mantida pelos fabricantes do equipamento;
- Fornecer acesso ao site web de suporte dos fabricantes do equipamento para verificar o andamento dos chamados de suporte abertos para os componentes da solução;

Solução de microssegmentação

Conforme pode ser observado no relatório do Gartner sobre o mercado de microssegmentação 3790056, existem alguns fabricantes atuantes neste nicho de tecnologia. Segue uma breve análise das alternativas.

1) Opção de microssegmentação implantada em software livre:

Não existem alternativas em software livre que resolvam o problema solucionado com microssegmentação, tampouco não há soluções disponíveis no Portal do Software Público Brasileiro.

2) Opção de microssegmentação baseada em cliente instalado nas máquinas:

Existem algumas soluções no mercado de microssegmentação baseada em clientes, tais como:

- GuardCore (Akamai);
- CISCO Secure Workload;
- Illumio.

Verificando em homologações e processo públicos, foi identificado um processo licitatório do SENAC-DF recém homologado, a saber, PE 41/2023, do qual saiu vencedor fabricante Guardcore.

Este tipo de solução, independente de fabricante, utiliza-se de um cliente a ser instalado em todos os ativos do ambiente, e toda a segurança do produto se baseia nas ações deste agente. Ele consegue atender aos requisitos da microssegmentação, fazendo a proteção do tráfego leste-oeste, porém sem conseguir criar patches virtuais, uma funcionalidade extremamente relevante para a CSID.

3) Opção de microssegmentação sem instalação de cliente nas máquinas:

Foi identificada a solução de microssegmentação da fabricante VMware denominado NSX, em diversos procedimentos licitatórios, a exemplo do CNJ (Contrato 02/2023), Senado (pregão 14/2022), ANEEL (pregão 22/2021), STM (pregão 72/2022) e Prefeitura do Rio de Janeiro (545/2022).

Esta solução é da fabricante VMware. Como todo o ambiente de virtualização do Superior Tribunal de Justiça é deste fabricante, a integração é nativa e transparente, sendo habilitada em nível de hipervisor e não necessitando instalar qualquer tipo de cliente nos dispositivos. Além disso, o NSX possibilita a criação de patches virtuais.

4.2 Análise e comparação entre os custos totais das soluções de TIC avaliadas:

Solução de microssegmentação

Os valores de contratações descritas nos quadros abaixo servem como comparação das soluções disponíveis no mercado.

- Licenciamento

Órgão	Pregão	Documento	Valor mensal por licença	Fabricante	Observação	SEI
CNJ	27/2022	Contrato 02/2023	R\$ 629,34	VMware	Valor total de R\$ 725.000,00 para 32 licenças e suporte por 36 meses.	4267549
						4087434
Senado	14/2022	Termo de Homologação pregão 14/2022	R\$ 958,94	VMware	Valor para 8 licenças e suporte por 36 meses: R\$276.174,40 (item 2)	4308728
SENAC	41/2023	Termo de Homologação pregão 41/2023	R\$ 552,11	Akamai	Valor total de R\$ 295.000,00 para 50 licenças, mais suporte por 12 meses por R\$ 36.270,00	3801247
MME - ANEEL	22/2021	Termo de Adjudicação pregão 22/2021	R\$1.040,18	VMware	Valor total de R 2.496.440,00, para 40 licenças e suporte por 60 meses.	4267560
TJGO	60/2021	Contrato 202112000311031	R\$ 713,70	VMware	Valor total de R\$ 1.926.999,75, para 75 licenças e suporte por 36 meses.	4341997
STJ	-----	Proposta Comercial Akamai	R\$ 348,00	Akamai	Valor total de R\$ 12.528.000,00, para 600 licenças (por máquina virtual do STJ) e suporte por 60 meses.	3801258
STJ	-----	Proposta Comercial OST	R\$ 185,83	VMware	Valor total de R\$ 6.743.520,00, para 1008 licenças (por core do vCenter do STJ) e suporte por 36 meses.	4217151
STJ	-----	Proposta Comercial YSSY	R\$ 166,03	VMware	Valor total de R\$ 6.024.942,00, para 1008 licenças (por core do vCenter do STJ) e suporte por 36 meses.	4217152
STJ	-----	Proposta Comercial PPN	R\$ 188,62	VMware	Valor total de R\$ 6.844.521,60, para 1008 licenças (por core do vCenter do STJ) e suporte por 36 meses.	4217153
STJ	-----	Proposta Comercial Decision	R\$ 166,82	VMware	Valor total de R\$ 6.053.632,20, para 1008 licenças (por core do vCenter do STJ) e suporte por 36 meses.	4217156

*Colocando como referência a licença Enterprise Plus por processador do NSX.

- Valor unitário da instalação

Órgão	Pregão	Documento	Valor unitário da instalação	Observação	SEI
MME - ANEEL	22/2021	Termo de Adjudicação pregão 22/2021	R\$ 171.360,00	Valor de R\$ 357,00 por hora. Colocando-se uma estimativa de 480 horas para a implementação	4267560
STJ	-----	Proposta Comercial Guardcore	R\$ 1.440.000,00	Valor da proposta	3801258
STJ	-----	Proposta Comercial OST	R\$ 320.869,00	Valor da proposta	4217151
STJ	-----	Proposta Comercial YSSY	R\$ 336.912,45	Valor da proposta	4217152
STJ	-----	Proposta Comercial PPN	R\$ 310.900,00	Valor da proposta	4217153
STJ	-----	Proposta Comercial Decision	R\$ 338.516,80	Valor da proposta	4217156

*Colocando como referência a Instalação e Configuração da solução de Microssegmentação

- Treinamento

Órgão	Pregão	Documento	Valor unitário por crédito	Observação	SEI
TJGO	60/2021	Contrato 202112000311031	R\$ 715,00	Considerando valor de 1,3 horas por crédito	4341997
STJ	-----	Proposta Comercial OST	R\$ 930,15	Valor da proposta	4217151
STJ	-----	Proposta Comercial PPN	R\$ 964,60	Valor da proposta	4217153
STJ	-----	Proposta Comercial Decision	R\$ 816,00	Valor da proposta	4217156

*Colocando como referência o treinamento da solução de microssegmentação

Foram avaliados processos licitatórios tanto para microssegmentação com o fabricante VMware quanto Akamai. É importante observar que a forma de licenciamento entre as soluções é diferente, sendo o NSX licenciado por "core" de processador, enquanto no Guardcore o licenciamento é por ativo instalado. Para efeitos de comparação, verificou-se o valor por licença por mês, já que os períodos de contemplação dos processos avaliados são muito variantes, desta forma, busca-se uma parâmetro de referência condizente com todas os processos identificados.

Não se observa uma diferença considerável entre as tecnologias, sendo relativamente equilibrados os valores para os dois tipos de fabricantes considerados, existindo aquisições de NSX mais caras e mais baratas do que do Guardcore.

4.3 Avaliação das necessidades de adequação do ambiente do Tribunal:

Solução de microssegmentação

A depender da solução adotada, pode ser necessária a instalação de clientes em todas as máquinas, ou ainda, pode ser necessária a instalação de complementos no ambiente VMware do Tribunal, a depender da solução adquirida.

A solução proposta visa evitar a necessidade de instalação de clientes em todas as máquinas, pois isso poderia causar um fragilidade na segurança e uma sobrecarga na instalação, configuração e gerenciamento desse novo item de configuração. O Tribunal já dispõe de ambiente específico para instalação e implantação da solução escolhida, ambiente VMware de virtualização, e a solução NSX é nativa e recomendada pelo fabricante para esse tipo de implementação, uma vez que há completa compatibilidade e especialmente não há necessidade de instalação de clientes nas máquinas. Isto posto, somente é necessário instalar e licenciar essa funcionalidade no sistema operacional dos hipervisores (ESXi), sendo, portanto, totalmente transparente e com impacto mínimo na infraestrutura do Tribunal.

4.4 Justificativa da solução de TIC escolhida, considerando o ciclo de vida do objeto:

Solução de microssegmentação

Esta equipe de planejamento da contratação entende que a opção 3 - Microssegmentação sem cliente - é a solução mais adequada para as necessidades do STJ.

Deve-se levar em consideração que todo o ambiente de virtualização do Tribunal funciona em uma estrutura de vCenter da Fabricante VMware, conforme contratos de hiperconvergência atualmente vigentes com a fabricante Dell, 108/2020 (2309385), 033/2020 (1965909), 107/2020 (2282866) e 028/2020 (1943952). Trata-se de contratações extremamente críticas para o STJ, pois hospedam toda a estrutura de virtualização de Datacenter, envolvendo em absoluto todos os sistemas ofertados pela Corte aos servidores, colaboradores e cidadãos. Importante observar ainda que esta estrutura tende a aumentar, já que há previsão no orçamento de 2024 para a ampliação do ambiente VMware do STJ, conforme proposta no PCaQ sob o código STI2024-032 - Licenças de virtualização VMware.

Destaca-se que a fabricante VMware é reconhecidamente líder e pioneira no mercado de virtualização e de soluções de hiperconvergência - correspondendo exatamente na estrutura de virtualização adotada pelo Superior Tribunal de Justiça -, conforme pode-se observar nas imagens a seguir do Gartner.

Figure 1: Magic Quadrant for Hyperconverged Infrastructure Software

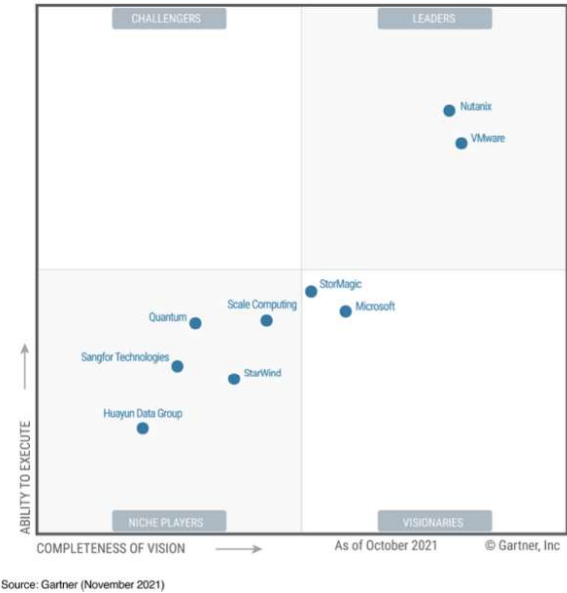


Figure 1. Magic Quadrant for x86 Server Virtualization Infrastructure



Trata-se de uma empresa já consolidada mundialmente, no mercado brasileiro presente desde 2002, oferecendo inclusive suporte telefônico e portal em português do Brasil.

A VMware é a fabricante da solução de virtualização do Datacenter do Tribunal, e a única fabricante capaz de ofertar uma solução de microssegmentação completamente sem clientes. Para tanto, a VMware dispõe do produto NSX, totalmente nativo e aderente ao vCenter, sendo esta a recomendação da fabricante como ferramenta a se adotar para uma virtualização em nível de rede e microssegmentação efetiva. Uma vez que toda a infraestrutura de virtualização do Superior Tribunal de Justiça se sustenta por produtos da fabricante VMware, esta Equipe de Planejamento da Contratação entende ser o mais adequado e natural que a alternativa para virtualização de redes e microssegmentação seja ofertada pela mesma fabricante, garantido completa padronização e compatibilidade.

O VMware NSX tem mais de 17.000 clientes e 91% da Fortune 100, reconhecida como solução número um para SDN e SDWAN, conforme quadrante mágico do instituto Gartner.

Figure 1: Magic Quadrant for SD-WAN



Com o NSX, é possível de fato fazer uma microssegmentação e isolamento em nível de máquina virtual, sem necessidade de instalar nada nos ativos. Somente é necessário instalar e licenciar a funcionalidade NSX no vCenter, sendo totalmente transparente aos usuários.

Uma solução de microssegmentação por agentes, por mais que seja interessante e que funcione adequadamente, a simples necessidade de instalar esse cliente já torna a implementação totalmente dependente deste agente. Desta forma, apesar de não haver POCs de conhecimento público no momento da confecção deste Estudo Técnico Preliminar, entende-se que este é um possível vetor de ataque a ser eventualmente explorado por hackers com o objetivo de "quebrar" a microssegmentação. Um cibercriminoso poderia se utilizar de técnicas para evadir, parar, danificar o agente de microssegmentação, afinal, trata-se de um programa instalado no sistema operacional, consequentemente, pode ser explorável por eventuais vulnerabilidades. É um risco inerente à solução. Para o caso da microssegmentação sem agentes, no entanto, este risco é absolutamente inexistente, já que não há que se falar em nada instalado em nível de sistema operacional nas máquinas virtuais; a microssegmentação é completamente transparente e nem é possível identificar que existe uma solução implementada de microssegmentação em um eventual caso de comando e controle da máquina, pois nada há instalado. Não há, portanto, qualquer possibilidade de exploração tampouco viabilidade de se "burlar" o serviço, sendo, pois, o mais seguro possível.

Outro ponto importante na definição do produto de microssegmentação NSX da fabricante VMware é que não há qualquer tipo de cerceamento de competição, uma vez que existe uma grande quantidade de fornecedores aptos e homologados a comercializar o software, conforme pode ser validado no site do fabricante: [https://partnerlocator.vmware.com/#sort=relevancy&f:@sfaccountcountryc=\[BRAZIL\]](https://partnerlocator.vmware.com/#sort=relevancy&f:@sfaccountcountryc=[BRAZIL]).

Ademais, conforme estabelece o Art. 41 da Lei 14.333:

- Art. 41. No caso de licitação que envolva o fornecimento de bens, a Administração poderá excepcionalmente:
- 1 - indicar uma ou mais marcas ou modelos, desde que formalmente justificado, nas seguintes hipóteses:

a) em decorrência da necessidade de padronização do objeto;

b) em decorrência da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração;

Entende-se que apenas a fabricante VMware consegue entregar a solução de microssegmentação conforme opção 3 (sem agente).

Fazendo-se um paralelo entre a opção 2 (microssegmentação com agente) e a opção 3 (microssegmentação sem agente) - listadas na seção 4.1 deste Estudo Técnico Preliminar:

Microssegmentação com agente instalado:

- É necessário instalar um agente no sistema operacional, agente este que funciona também como um firewall de máquina. Qualquer agente instalado está sujeito a ataques do tipo "tampering", ou seja, tentativas de ser desabilitado ou evitado por um atacante, perdendo assim todas as políticas de segurança implementadas;
- o deploy dos agentes exige scripting para cada workload/VM. A atualização do cliente não é necessariamente automática, depende de ferramentas externas para orquestração e automação.
- O agente pode apresentar picos de uso de CPU e memória, dependendo do perfil de tráfego, competindo com os processos efetivamente servidos pela máquina virtual e eventualmente podendo onerar na performance da máquina;
- O licenciamento ocorre por hospedeiro, ou seja, por VM, Node ou Bare Metal. Isso implica que o licenciamento pode ser afetado com o crescimento natural do datacenter. Com as estratégias atuais de virtualização, o surgimento de novas máquinas para estratégias de escalabilidade e algo extremamente natural e inerente à solução, sendo que a implicação de problemas de funcionamento da solução em virtude de novas máquinas é algo completamente inadmissível;
- As soluções com agentes não conseguem se integrar nativamente e por completo com as ferramentas do ambiente VMware do Datacenter, como vRealize Automation, VCenter, Ansible Modules ou Terraform Provider;
- Em geral as soluções com clientes não auxiliam diretamente em estratégias de Recuperação de Desastres ou de Planos de Continuidade (por exemplo, realizando a extensão em nível de camada 2 para um site diferente em caso de recuperação de desastre ou para contingência).
- O firewall implementado com o agente opera até a camada 4 do modelo OSI.

Microssegmentação sem agente instalado:

- A instalação e configuração ocorrem de forma ultra-rápida, não requer instalação de agentes ou reinicialização das máquinas protegidas;
- Não há necessidade de processos para gestão e distribuição do software cliente nas máquinas, reduzindo-se a carga de trabalho na administração e validação da solução, e garantindo a completa adequação de todo o Datacenter, pois não há possibilidade de se "evitar" o processo;
- A solução da VMware, NSX, sem agente, é executada diretamente no core do hypervisor, completamente fora da superfície de ataque, em uma arquitetura completamente "agentless";
- O NSX mantém a persistência das políticas de microssegmentação mesmo com a perda da camada de gerência;
- Não requer hardware dedicado para as funções de gerenciamento do ambiente local, e não depende de conexão com serviços de nuvem para a administração;
- Implementa o Zero Day VM least privilege, ou seja, toda VM ou Container provisionado já nasce dentro de uma política de segurança do NSX;
- O NSX firewall é uma solução de firewall statefull com IDS e IPS sem necessidade de overlay ou de haipin do tráfego para um appliance externo;
- A performance do ambiente fica totalmente indiferente com a instalação do NSX;
- O NSX firewall term performance de firewall line-rate com praticamente zero latência e alto desempenho por host;
- A console NSX Manager centraliza o gerenciamento dos NSX Firewalls distribuídos entre todos os ambientes;
- O NSX Firewall opera até a camada 7 do modelo OSI.
- Incluso no licenciamento a funcionalidade "NSX Intelligence", que realiza discovery automático das aplicações e suas dependências e facilita a criação das políticas de segurança via Netflow;
- Completa e nativa integração com o ambiente VMware VCenter, vRealize Automation e demais módulos do fabricante;
- O licenciamento ocorre baseado nos núcleos de processadores do Datacenter, totalmente indiferente à quantidade de máquinas virtuais, sendo, pois, completamente aderente à estratégias de escalabilidade do ambiente, não atrapalhando em nada na necessidade de criação de novas máquinas e novos workloads;
- Evita riscos com possíveis incompatibilidades entre agentes e Sistemas Operacionais e, ou com outros agentes já aplicados – Antivírus, backup, etc;
- Resiliência: a microssegmentação está fora da superfície de ataque, isto é, se eventualmente a carga de trabalho é comprometida por um malware, o Firewall distribuído não é afetado;
- Alinhado com a arquitetura de nuvem, onde ao se criar aplicações a segurança já está embarcada;
- Reduz muito o custo operacional, pois livra o time de infraestrutura da necessidade de validar, instalar e manter milhares de novos agentes no ambiente. Facilitando o processo de gerência e troubleshooting;
- Curva de custos. O crescimento exponencial de novas aplicações cada vez mais fragmentadas em pequenas cargas de trabalho, leva o custo da solução baseada em agentes às alturas pois cada máquina virtual ou container necessita de uma licença;
- O formato de licenciamento permite que o custo se eleve de forma alinhada com o crescimento do ambiente computacional e não às aplicações. Dessa forma, nosso modelo de licenciamento não deve ser comparado de forma direta com outros baseados em agentes;
- Segurança avançada. A microssegmentação reduz muito a exposição do ambiente, mas por si só já não é suficiente para protegê-lo por completo, isto porque há outros métodos de ataque que agem onde esta solução não alcança, a Plataforma NSX oferece funções avançadas de segurança que complementam a microssegmentação: IDS/IPS distribuído de simples implementação – facilidade que pode ser adicionada ao próprio Firewall distribuído do NSX, Sandbox, Network Threat Analysis sem a necessidade de TAPs externos e anti-malware, são facilidades que podem também se somarem ao NSX, elevando a segurança a outro patamar;
- É a primeira solução na categoria de NDR reconhecida com o selo AAA do SE LABs, onde 100% das ameaças puderam ser identificadas com zero por cento de falso positivo;
- Para ambientes de DevOps o NSX possui facilidades importantes como Service Mesh, que oferece para o ambiente de microserviço, observabilidade e análise de segurança, vulnerabilidades e reputação.

4.4.1 Ciclo de vida do objeto:

- As versões das licenças e softwares que compõem a solução deverão ser ofertadas novas, sem uso anterior, e deverão permanecer com previsão de suporte do fabricante pelos próximos 36 (trinta e seis) meses, a contar da data de homologação do certame.
- Para microssegmentação, todo o ambiente do Tribunal deve ser licenciado, inclusive com a previsão de crescimento do ambiente de virtualização durante o prazo da contratação.
- As versões das licenças e softwares deverão ser do tipo Enterprise, com suporte 24x7.
- O prazo para entrega desses bens é de, no máximo de 30 (trinta) dias corridos a contar da assinatura do contrato.
- Os bens deverão ser entregues (caso necessária a entrega de algum bem fisicamente) no endereço Setor de Administração Federal Sul - SAFS, Quadra 06, Lote 01, Bloco F, Prédio da Administração, subsolo, Brasília-DF, CEP 70095-900, no horário das 9h às 18h.
- Será necessário apresentar um Plano de Implantação dos produtos e serviço de instalação e configuração, no prazo de 30 (trinta) dias, a contar da assinatura do contrato.
- Após entrega dos produtos, será realizada a instalação e configuração dos softwares e licenças em plena compatibilidade com o ambiente computacional do STJ, no prazo máximo de 90 (noventa) dias corridos a contar da emissão do termo de recebimento provisório.
- A contratação também deverá prever serviço técnico de capacitação para servidores do Tribunal, bem como serviço técnico de implantação e operação assistida.
- A contratação também prevê serviço de suporte, que será iniciado imediatamente após a emissão do Termo de Recebimento Definitivo e se encerrará juntamente com o término do contrato (fim da vigência do contrato).
- A empresa deverá realizar os atendimentos presenciais no seguinte local Setor de Administração Federal Sul - SAFS, Quadra 06, Lote 01, Bloco F, Prédio da Administração, Brasília-DF, CEP 70095-900;
- O Suporte emergencial disponível presencialmente ou em regime de plantão, nesse caso podendo ser acionado para atendimento de acordo com os níveis de prioridades, nas mesmas condições do monitoramento de ambiente.
- A empresa deverá disponibilizar número telefônico, com atendimento ininterrupto 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, para fins de abertura de chamados técnicos, assim como para acompanhamento da solução de problemas. Os chamados de suporte são priorizados por nível de urgência de solução. O atendimento deverá ocorrer preferencialmente em português do Brasil.
- Em relação à gestão de resíduos, será necessário dar destinação ambientalmente adequada aos componentes da solução que foram substituídos pois apresentaram defeitos, quando chegarem ao final do seu ciclo de vida, conforme preconizado pela Política Nacional de Resíduos Sólidos (https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/112305.htm) e pelo Plano de Gestão de Resíduos Sólidos do STJ (https://www.stj.jus.br/static_files/STJ/Institucional/Educa%C3%A7%C3%A3o%20e%20cultura/socioeducativo/plano_gerenciamento_residuos.pdf).
- Em relação à gestão de resíduos, quando estes equipamentos chegarem ao final do seu ciclo de vida, será necessário também dar destinação ambientalmente adequada aos produtos conforme preconizado pela Política Nacional de Resíduos Sólidos (https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/112305.htm) e pelo Plano de Gestão de Resíduos Sólidos do STJ (https://www.stj.jus.br/static_files/STJ/Institucional/Educa%C3%A7%C3%A3o%20e%20cultura/socioeducativo/plano_gerenciamento_residuos.pdf).

4.5 Sustentação do contrato:

Garantir o funcionamento do ambiente em relação à solução instalada pela CONTRATADA, incluindo todos os serviços, configurações e fornecimento de “firmwares”, “fixes” e “releases”, durante toda a vigência do contrato.

Realizar manutenções evolutivas, que consiste na atualização de versão dos softwares, fornecendo, instalando e configurando as novas versões, releases e/ou upgrades lançados durante a vigência contratual, mantendo-os funcionais e compatíveis com o ambiente utilizado pelo STJ;
Realizar manutenções preventivas por meio de visitas técnicas mensais para verificar a “saúde” da solução, monitorar os serviços, verificar configurações e sugerir melhorias (pode ser feito de forma remota);
Disponibilizar e tornar disponível à CONTRATANTE uma estrutura de suporte técnico, através de meio telefônico ou outro recurso de comunicação que se faça disponível e conveniente às partes, para realização de manutenções corretivas, esclarecimento de dúvidas e orientação com relação ao produto;
Promover o isolamento, identificação e caracterização de falhas de laboratório (bugs), encaminhamento da falha ao laboratório do fabricante e acompanhamento de sua solução;

Os serviços de suporte técnico deverão estar disponíveis durante os 07 (sete) dias da semana, 24 (vinte e quatro) horas por dia, executando-os sempre que aberto um chamado técnico pelo STJ;

Cumprir a execução dos serviços de suporte técnico e atualização de versões, sempre que necessário, em tempo, forma e regime de horário devidamente estabelecidos pelo STJ;
As intervenções que possam causar indisponibilidades devem ser executadas em horários previamente acordados, e fora do horário de expediente do Tribunal.

Entregar o Plano de Implantação da solução em, no máximo, 30 dias corridos da assinatura do contrato, para validação do CONTRATANTE;

- Realizar a entrega das licenças no prazo máximo de 30 (trinta) dias corridos após assinatura do contrato;
 - O Termo de Recebimento Provisório será emitido em até 05 (cinco) dias corridos após a entrega da solução;
 - Realizar a instalação e configuração da solução em no máximo 90 (noventa) dias corridos após a emissão do Termo de Recebimento Provisório;
 - O Termo de Recebimento Definitivo será emitido em até 10 (dez) dias corridos após a comunicação da CONTRATADA informando o término da instalação e configuração da solução;
- O serviço de Suporte Técnico se iniciará imediatamente após a emissão do Termo de Recebimento Definitivo e se encerrará juntamente com o término do contrato.

Quanto aos recursos humanos a solução será sustentada pelos servidores da Coordenadoria de Segurança da Informação e Defesa Cibernética – CSID – juntamente com os profissionais do SOC, objeto do Processo STJ n. 022086/2022. Oportunamente, servidores e colaboradores da CIEP também poderão contribuir na sustentação da solução.

Quanto aos recursos materiais, não serão necessários novos recursos uma vez que a solução pretendida é basicamente de software.

Na hipótese de interrupção contratual, não haverá prejuízo imediato na continuidade do negócio, uma vez que o licenciamento é feito diretamente com o fabricante.

Haverá prejuízo referente ao serviço de suporte. Entretanto, o contrato do SOC deverá dar continuidade à gestão da solução e resolução de problemas técnicos de menor complexidade, enquanto não houver suporte de um fornecedor autorizado. Por fim, nesse caso, um novo suporte técnico deverá ser contratado.

I) Atividades de encerramento contratual, consistirá em:

- a. Entrega das últimas versões da solução fornecidos pelo fabricante, que poderá ser feito por meio de uma URL – Uniform Resource Location – para download;
- b. Apresentação de relatório sobre o estado da solução com indicações de possíveis problemas e recomendações;
- c. Remoção dos acessos das contas de suporte da empresa contratada;
- d. Não se aplica ao objeto a devolução de recursos materiais ou eliminação de caixas postais;

II) A transição contratual incluirá, pelo menos, as seguintes atividades:

- a. Inclusão no plano de aquisições de previsão de contratação ou renovação da solução;
- b. Elaboração e acompanhamento do processo de contratação, com os artefatos necessários;

O STJ possui independência em relação à contratada no que diz respeito à gestão e uso regular da solução. O suporte visa resolver problemas relacionados ao mal funcionamento da solução, ou seja, defeitos ou vícios de fabricação.

Entretanto, nesse sentido, não há nenhum vínculo com uma contratada específica, o serviço de suporte pode ser prestado por qualquer empresa que represente oficialmente o fabricante no Brasil.

Não é possível, contudo, independência em relação ao tipo de solução. O STJ não possui capacidade técnica para substituir soluções de microsegmentação por alguma solução desenvolvida internamente ou disponibilizada por outros órgãos do Governo brasileiro.

Considerando ainda que não é uma solução desenvolvida sob demanda, a CONTRATADA deverá prover opções de transferência de conhecimento aos servidores e colaboradores de Tribunal, nos moldes estabelecidos no item 3.2 deste Estudo Técnico Preliminar.

Por fim, dado a natureza da solução, não haverá durante a vigência contratual, produtos gerados ao longo do contrato que requeiram proteção de direitos de propriedade intelectual.

4.6 Estimativa das quantidades a serem contratadas:

Quantidade:

O licenciamento da solução de microsegmentação deve englobar toda a estrutura de Datacenter do Superior Tribunal de Justiça, ou seja, todo o ambiente deve estar apto a utilizar a microsegmentação. Atualmente o Datacenter do STJ possui 18 hosts de 2 processadores, cada processador com 28 núcleos (cores). O total de cores em todo o ambiente é 18*2*28 = 1008 cores. Este é o licenciamento para o caso do produto NSX da VMware.

Como todo o ambiente de Datacenter do STJ já utiliza a fabricante VMware, é recomendado que se mantenha com uma solução deste mesmo fabricante, licenciando todo o ambiente de VMware do Tribunal.

O dimensionamento para o treinamento se baseou no catálogo oficial de cursos da fabricante VMware, documento SEI 4057423. A previsão é que sejam treinados 6 (seis) servidores do Tribunal - dois da CSID, dois da SEPLA e dois da SECTE.

Pretende-se realizar os treinamentos "NSX -T Data Center: Install, Configure, Manage" (23 créditos), "NSX-T Data Center for Intrinsic Security" (23 créditos).

Considerando-se a estimativa de turmas fechadas para 6 (seis) servidores, o total de créditos estimados é (23+23) *6, resultando em 276 créditos estimados. Como estes treinamentos podem sofrer variações no quantitativo de créditos, atualizações, ou mesmo o interesse do Tribunal pode alterar, são estimados 300 (trezentos) créditos para treinamento de soluções da VMware.

Marca/Modelo:

Como todo o ambiente de Datacenter do STJ já utiliza a fabricante VMware, é recomendado que se mantenha com uma solução deste mesmo fabricante, licenciando todo o ambiente de VMware do Tribunal.

Data Prevista:

Dezembro de 2024

4.7 Estimativa do valor da contratação:

GRUPO	ITEM	DESCRIÇÃO	QTD.	VALOR UNITÁRIO (R\$)	VALOR TOTAL(R\$)
1	1	VMware NSX Data Center Enterprise Plus por 36 meses com Advanced Threat Prevention (por core)	1008	R\$ 5.977,08	R\$ 6.024.896,64
	2	Serviço de instalação e configuração do solução de microsegmentação NSX	1	R\$ 295.711,65	R\$ 295.711,65
	3	Crédito de treinamento	300	R\$ 856,44	R\$ 256.932,00
TOTAL					R\$ 6,577.540,29

Solução de microsegmentação

- Item 1 (licenciamento)

Na pesquisa de preços (4342410) o menor valor por *core* por mês foi de R\$166,03. Multiplicamos este valor por 36 meses e pelos 1008 cores existentes nos datacenters do STJ:

$166,03 \times 36 \times 1008 = R\$ 6.024.896,64.$

- Item 2 (Instalação e configuração NSX)

Estima-se um montante de 480 horas para realizar a instalação e configuração da solução. Para o caso da ANEEL, utilizou-se o item 03 do contrato, contemplando horas técnicas para consultoria, serviços especializados, projetos de planejamento, instalação e configuração da solução (cálculo está na tabela acima). O valor estimado foi de R\$ 295.711,65, conforme 4342410.

- Item 3 (Crédito de treinamento)

Para utilizar a contratação do TJGO como referência para este item, considera-se uma estimativa de 23 créditos para um curso de 30 horas, conforme catálogo oficial da fabricante VMware: 4057423. Desta forma, um crédito equivale aproximadamente a 30/23 = 1,3 horas. O item 11 do TJGO contempla também a utilização de horas técnicas para realização de treinamento, por isso é razoável a utilização deste item nesta estimativa de preços (cálculo na tabela acima). O valor estimado foi de R\$ 856,44 por crédito, $R\$ 856,44 \times 300 = R\$ R\$ 256.932,00.$

4.7.1. Responder este item somente para as contratações abaixo de R\$ 80.000,00 (se a adjudicação for por item, esse valor deve ser considerado para cada item):

(X) NÃO SE APLICA

() A licitação pode ser destinada exclusivamente à empresas ME/EPP conforme estabelece o inciso I do art. 48 da [LC 123/2006](#).

() A licitação deverá ser de ampla participação em razão de não haver um mínimo de 3 (três) fornecedores competitivos enquadrados como microempresas ou empresas de pequeno porte sediados local ou regionalmente e capazes de cumprir as exigências estabelecidas no instrumento convocatório. **Justificativa:** *"o usuário deverá demonstrar essa excepcionalidade na instrução processual."*

() A licitação deverá ser de ampla participação em razão do tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte não ser vantajoso para a administração pública ou representa prejuízo ao conjunto ou complexo do objeto a ser contratado. **Justificativa:** *"o usuário deverá demonstrar essa excepcionalidade na instrução processual."*

() Não se aplica em razão da licitação ser dispensável ou inexigível.

4.8 Justificativa para o parcelamento ou não da solução:

() Não se aplica em razão da licitação ser dispensável ou inexigível.

() Não é possível o parcelamento, pois trata-se de apenas 1 (um) item. (ADJUDICAÇÃO: MENOR PREÇO POR ITEM).

() É possível a contratação da solução de forma divisível observado o §2 do art. 40 da [Lei n. 14.133/2021](#) (ADJUDICAÇÃO: MENOR PREÇO POR ITEM).

(X) Todos ou alguns itens da solução devem ser agrupados para o fornecimento por uma única empresa, observado o §3 do art. 40 da [Lei n. 14.133/2021](#) (ADJUDICAÇÃO: MENOR PREÇO GLOBAL).

Justificativa:

A adjudicação será realizada por MENOR PREÇO GLOBAL.

Para se garantir a viabilidade técnico-administrativa dessa contratação, é fundamental que todos os itens a serem contratados, bem como os serviços decorrentes sejam adjudicados para um único licitante vencedor.

A definição pela contratação para uma única empresa levou em consideração o prejuízo de ordem técnica que poderia ocorrer caso os serviços fossem prestados por diferentes empresas, uma vez que os itens especificados a serem contratados guardam estreita relação entre si e dependem de forte integração para que sejam efetivos e alcancem os resultados pretendidos.

A orientação do TCU no Acórdão nº 861/2013 - Plenário: "São lícitos os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si", admite a possibilidade do agrupamento de itens em lote único nos pregões eletrônicos.

A contratação dos itens descritos em separado com diversas empresas sendo adjudicadas certamente poderá vir a representar alto risco para o CONTRATANTE, no sentido de que as diversas contratadas poderiam atribuir umas às outras o descumprimento de suas responsabilidades, tornando extremamente difícil a identificação de qual delas deveria sofrer um eventual processo sancionatório.

Além disso, corroborando essa necessidade de adjudicação conjunta de todos os itens, percebe-se que o mais conveniente para a CONTRATANTE é que todos os serviços previstos sejam realizados por uma única empresa, de forma a se evitar a multiplicidade de contratos, possibilitando uma melhor fiscalização e controle.

A execução dos serviços por mais de uma empresa acarretaria elevado custo à Administração e uma complexa rede de coordenação entre os projetos e contratos, o que poderia comprometer a qualidade e a efetividade dos resultados e dos contratos administrativos decorrentes, no caso da adoção de outra forma de adjudicação.

Portanto, para que se garanta total compatibilidade técnica do conjunto da solução, bem como uma maior racionalidade administrativa, a adjudicação por Menor Preço Global configura-se como a melhor alternativa para a CONTRATANTE.

4.9 Contratações correlatas e/ou interdependentes:

Esta contratação é correlata aos contratos 108/2020 - Subscrições VMware - SEI 033601/2020 e Contrato 033/2020, também referente à subscrições VMware, processo SEI 000075/2020.

4.9.1 Existe um contrato atual vigente ou instrumento equivalente, com objeto a ser licitado?

(X) Não. () Sim. O contrato atual (n. ____/20____) (Processo SEI n._____) terá sua vigência finda em ____/____/20____.

4.10 Alinhamento entre a contratação e o PCAq:

() O objeto pretendido não consta do PCAq. **Justificativa:**
(X) O objeto pretendido consta do PCAq2024 sob o código STI2024-066.000.

FONTE DE RECURSOS			
Planejamento das Aquisições e Contratações – PCAq 2023			
Codificação Sequencial	Descrição	Valor (R\$)	Impacto no indicador do PLS
STI2024-066	Micro segmentação	R\$ 2.079.841,32	Não se aplica
Proposta orçamentária			
Código de Execução	Descrição	Valor Planejado (R\$)	
Código TIC: 202320306 Elemento: 3.33.90.40.06	Micro segmentação - Plataforma de virtualização de redes	R\$ 2.079.841,32	
() Não há previsão orçamentária			

4.11 Alinhamento entre a contratação e outros instrumentos de planejamento da administração:

ALINHAMENTO ESTRATÉGICO		
Plano Estratégico Institucional – Plano STJ 2021 – 2026		
Perspectiva	Objetivo Estratégico	
Pessoas e Recursos	• Aprimorar a governança institucional; • Intensificar o uso de tecnologias da informação.	
Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC 2023 – 2024		
Objetivo Estratégico de TIC	Ações Táticas	Projeto
OE01 Evoluir e manter a infraestrutura de ativos tecnológicos; OE06 Fortalecer as estratégias de continuidade de TIC; OE10 Fortalecer a segurança da informação e a proteção de dados de maneira estruturada e contínua	AT01.01 Sustentar a infraestrutura de TIC e buscar soluções tecnológicas inovadoras; AT06.01 Aprimorar a continuidade de serviços de TIC; AT10.01 Aumentar a maturidade em Segurança da Informação no STJ.	PDTIC2024.PJ02 Aprimoramento das soluções de segurança de SI
Plano Operacional de Tecnologia da Informação e Comunicação – PLANOP 2023 – 2024		
Código Operacional	Descrição	
PDTIC2024.AO02.07	Micro segmentação	
Plano de Contratações de Tecnologia da Informação e Comunicação – PCTIC 2023		
Número Sequencial	Justificativa da necessidade	
PCTIC-2023-062	A micros segmentação é uma técnica de segurança de rede que permite aos arquitetos de segurança dividir logicamente o data center em segmentos de segurança distintos até o nível de carga de trabalho individual e, em seguida, definir controles de segurança e fornecer serviços para cada segmento separadamente.	

4.12. Classificação do objeto:

Natureza:

(X) bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado;
() bens e serviços especiais: aqueles que, por sua alta heterogeneidade ou complexidade, não podem ser considerados bens e serviços comuns. **Justificativa:**

Tipo de bem:

(X) O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme art. 2º, II e III, do Decreto nº 10.818, de 27 de setembro de 2021, e art. 22, II e III, da Instrução Normativa STJ/GDG n. 4/2023.
() O objeto desta contratação se enquadra como sendo de bem de luxo, conforme art. 2º, I, do Decreto nº 10.818, de 27 de setembro de 2021, e art. 22, I, da Instrução Normativa STJ/GDG n. 4/2023. **Justificativa:**

Caracterização:

(X) Trata-se de serviço ou fornecimento contínuo, definido pela [Instrução Normativa STJ/GDG n. 10 de 28 de abril de 2022](#), alterada pela [Instrução Normativa STJ/GDG n. 5 de 16 de fevereiro de 2023](#).
() Trata-se de serviço ou fornecimento contínuo, AINDA NÃO definido pela [Instrução Normativa STJ/GDG n. 10 de 28 de abril de 2022](#). Nesse caso, o enquadramento deve ser autorizado pelo Diretor-Geral.
() O objeto é caracterizado como serviço não contínuo ou contratado por escopo, aquele que impõem ao contratado o dever de realizar a prestação de um serviço específico em período predeterminado, com valor acima do limite previsto para a dispensa de licitação (art. 75, incisos I e II da [Lei 14.133/2021](#)).

4.13 Participação de empresas reunidas em consórcio:

(X) Não será permitida a participação de empresas reunidas em consórcio. **Justificativa:** O objeto a ser contratado não possui condições técnicas complexas que exijam a atuação de mais de uma empresa para prestação dos serviços, uma vez que não exige junção de esforços de segmentos distintos destinados à sua prestação. Trata-se de serviços comumente prestados por diversas empresas que atuam individualmente no mercado.
() Será permitida a participação de empresas reunidas em consórcio. **Justificativa:** _____

4.14 Participação de pessoa física:

(X) Não.
() Sim. **Justificativa:** _____

5. Planejamento

5.1 Resultados pretendidos:

- Redução da superfície de ataque;
- Aumento da segurança do ambiente de datacenters;
- Prevenção contra ataques internos;
- Prevenção contra movimentação lateral;
- Isolamento de aplicativos;
- Aumento no desempenho da rede;
- Melhoria na detecção de atividades maliciosas;
- Redução de riscos e custos associados à falhas de segurança;
- Possibilidade de aplicação de patches virtuais em ativos que não podem ser devidamente atualizados;
- Redução no gasto de energia com estações de trabalho ligadas 24x7;
- Aumento da produtividade dos usuários remotos;
- Melhor gerência dos acessos remotos;

- Maior segurança dos acessos remotos.

5.2 Providências a serem adotadas pela Administração para início da execução do objeto:

Não há providências específicas a serem adotadas pela Administração no que concerne a esta Contratação.

5.3 Possíveis impactos ambientais:

I – Critérios:

5.3.1 Tenho conhecimento de que: A fabricante e/ou distribuidora, e/ou importadora, e/ou comerciante e/ou consumidora deste objeto deve possuir Cadastro Técnico Federal de Atividades Potencialmente Poluidoras e/ou Utilizadoras de Recursos Ambientais (CTF/APP)?

a) ☐ Não. ☐ Sim. Identifique a(s) categoria(s) da Ficha Técnica de Enquadramento (FTE): _____

b) (☒) a fabricante, e/ou distribuidora, e/ou importadora, e/ou comerciante, e/ou consumidora deste objeto **não se enquadra nas FTEs do CTE/APP**

5.3.2 Os produtos/objetos são constituídos de material (marque quantos itens forem necessários):

☐ renovável ☐ reciclado ☐ atóxico ☐ biodegradável ☒ não se aplica

5.3.3 Os objetos são considerados produtos perigosos (item 3 do Plano de Gestão de Resíduos Sólidos do STJ):

(X) Não. () Sim. Quais? _____

5.3.4 Os objetos da aquisição devem estar em conformidade com os seguintes regulamentos técnico/legal: (marque quantos itens forem necessários):

() Etiqueta Nacional de Conservação de Energia () Certificado de Conformidade de Potência Sonora de Produtos Eletrodomésticos () Certificado de Vistoria de Veículo () Ficha de Informações de Segurança de Produtos Químicos () Documento de Origem Florestal () Autorização para o Exercício da Atividade de Revenda de GLP () Outro(s). Especificar:

5.3.5 Há outros critérios de sustentabilidade, além dos relacionados acima:

(X) Não. () Sim. Descreva:

Deverão ser consideradas nesse item as diretivas do Guia de Licitações Sustentáveis do STJ, normativos internos e a legislação vigente.

II – Plano de Logística Sustentável do STJ (PLS-STJ):

5.3.6 Essa aquisição ou contratação demandará ou resultará em (marque quantos itens forem necessários)

- () geração de resíduo.
- () consumo de papel.
- () consumo de outros materiais de expediente (caneta, grampos, clips, pastas etc).
- () consumo de café ou açúcar.
- () consumo de água mineral envasada.
- () gastos com correspondências.
- () instalação de computador ou impressora.
- () aparelho de telefone fixo ou móvel.
- () consumo de energia elétrica.
- () consumo de água.
- () serviços de engenharia (instalações elétricas, hidráulicas, ponto de rede, ponto de telefone, divisórias).
- () obras civis (reforma ou construção de edificação).
- () serviço de limpeza - aumento da área a ser limpa no STJ.
- () serviço de vigilância - aumento no número de postos.
- () quantidade de veículos na frota do STJ.
- () gasto com contratos de veículos (manutenção, peças, insumos, seguro, lavagem, terceirização, exceto motorista)
- () consumo de combustível.
- () ação de qualidade de vida.
- () ação de capacitação socioambiental.
- (X) não demandará ou resultará em nenhum dos itens acima.

Esses itens referem-se aos temas monitorados pelo PLS-STJ. A partir da seleção do item, o gestor do indicador será comunicado para ciência dos impactos gerados e eventual inclusão no respectivo plano de ação.

III – Resíduos:

5.3.7 Gestão de resíduos (Caso tenha marcado “geração de resíduo” na pergunta anterior – Lei n. 12.305/2010 e Lei Distrital n. 5.418/2014)

a) Descreva os resíduos que serão produzidos (incluindo estimativa de quantidade, quando possível):

b) Há previsão de destinação final ambientalmente adequada desses resíduos?

(X) Não. () Sim. Pela CONTRATADA. () Sim, pelo STJ.

Descreva a destinação (se pela contratada, analisar os possíveis custos):

c) Você identifica outros impactos ambientais, além dos indicados acima? (art. 7º, inciso XII, [IN ME nº 40/2020](#)):

(X) Não, () Sim.

Descriva:

6. Viabilidade

6.1 Existe Ata de Registro de Preços em vigor que pode atender a demanda?

(X) Não () Sim Justificar a viabilidade técnica e econômica para a adesão:

6.1.1 A demanda poderá ser atendida por Ata de Registro de Preços?

() Não. (X) Sim. Justificar:

Está previsto para o ano de 2024, conforme PCAq 2024, código STI2024-032, uma ampliação no licenciamento do ambiente de VMware do Tribunal, inclusive com previsão de aquisição de novos servidores. Para que a solução de microssegmentação englobe essa provável expansão, a utilização de uma ata de registro de preço pode ser conveniente, de forma a garantir que os novos equipamentos eventualmente adquiridos sejam devidamente licenciados.

6.2 Previsão de recursos para a demanda:

(X) A contratação foi prevista na Proposta Orcamentária de 202320306, na Ação: Micro segmentação - Plataforma de virtualização de redes

() Não houve previsão orçamentária para contratação

6.3 Declaração de viabilidade:

A Equipe de Planejamento da Contratação declara a adequação da solução à necessidade e à realidade do Tribunal, sendo essencial para manutenção e bom funcionamento das soluções de TIC do Tribunal, de forma segura e eficiente.

7. Do Acesso às informações contidas no presente Estudo Preliminar:

Nos termos da [Lei n. 12.527, de 18 de novembro de 2011](#), esta unidade ou Equipe de Planejamento entende que:

() As informações contidas no presente Estudos Técnico Preliminar **DEVERÃO SER PÚBLICAS**, estando disponíveis para qualquer interessado, pois não se caracterizam como sigilosas.

(x) As informações contidas no item 2.1. do presente Estudo Técnico Preliminar **ASSUMEM CARÁTER SIGILOSO**, nos termos do art. 23 da [Lei n. 12.527/2011](#), e, portanto, deverão ter acesso restrito. **Justificativa:** tratam-se de informações sobre o ambiente do Superior Tribunal de Justiça que poderiam ser exploradas por atacantes cibernéticos mal intencionados em um eventual ataque à infraestrutura do Tribunal.

() As informações contidas no presente Estudo Técnico Preliminar **ASSUMEM CARÁTER SIGILOSO**, nos termos do art. 23 da [Lei n. 12.527/2011](#), e, portanto, deverão ter acesso restrito. **Justificativa:**

8. Responsabilidade dos servidores ou equipe de planejamento da contratação responsáveis pela elaboração e conteúdo do ETP:	
Certificamos que somos responsáveis pela elaboração do presente documento que compila os Estudos Técnicos Preliminares e que este traz os conteúdos previstos na Lei n. 14.133/2021 .	
	Documento assinado eletronicamente por Winston Luiz de Oliveira Rodrigues , Técnico Judiciário, Área de Apoio Especializado - Tecnologia da Informação, em 29/10/2024, às 10:01, conforme art. 1º, III, "b", da Lei 11.419/2006.
	Documento assinado eletronicamente por Edimar Lisboa das Chagas , Coordenador de Segurança da Informação e Defesa Cibernética, em 29/10/2024, às 13:58, conforme art. 1º, III, "b", da Lei 11.419/2006.
	Documento assinado eletronicamente por Jessica Souto Ferreira , Assistente IV, em 29/10/2024, às 14:09, conforme art. 1º, III, "b", da Lei 11.419/2006.
	Documento assinado eletronicamente por Vitor Gabriel Jaime Paiva , Chefe da Seção de Segurança da Informação, em 29/10/2024, às 15:06, conforme art. 1º, III, "b", da Lei 11.419/2006.
	A autenticidade do documento pode ser conferida no site https://sei.stj.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador 5876937 e o código CRC FF756676 .