



ESTUDOS TÉCNICOS PRELIMINARES
SERVIÇOS DE TIC SEM MÃO DE OBRA

1. Informações Gerais

1.1 N. do Processo SEI: 005492/2024

1.2 Unidade Requisitante:

Coordenadoria de Segurança da Informação e Defesa Cibernética - CSID

1.3 Unidade Técnica:

Seção de Gestão de Acesso e Eventos de Segurança - SEGAE

Seção de Segurança da Informação - SESEG

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:

a) integrante requisitante:

Nome: Leandro Gabriel Bastos Ferreira Unidade: Coordenadoria de Segurança da Informação e Defesa Cibernética - CSID

Nome: Edimar Lisboa das Chagas Unidade: Seção de Operação de Segurança de TIC - SOSTI

b) integrante técnico:

Nome: Uriel Kádmo Nunes Torres Unidade: Seção de Gestão de Acesso e Eventos de Segurança de TIC - SEGAE

Nome: Vitor Gabriel Jaime Paiva Unidade: Seção de Segurança da Informação - SESEG

c) integrante administrativo:

Nome: Francisco Carlos Alvez Diniz Unidade: Seção de Gestão de Contratações de TIC - SCONT

Nome: Vanderlei Barbosa da Silva Unidade: Seção de Gestão de Contratações de TIC - SCONT

1.6 Responsável pela aprovação do Estudo Preliminar:

Nome: Humberto Fontoura Pradera

Secretaria/Assessoria: Secretaria de Tecnologia da Informação e Comunicação - STI

1.7 Fiscais e gestores:

Fiscais técnicos:

Nome: Uriel Kádmo Nunes Torres - Titular: CSID - Coordenadoria de Segurança da Informação e Defesa Cibernética

Nome: Vitor Gabriel Jaime Paiva - Suplente: CSID - Coordenadoria de Segurança da Informação e Defesa Cibernética

Fiscais requisitantes, se for o caso:

Nome: Leandro Gabriel Bastos Ferreira - Titular. Unidade: CSID - Coordenadoria de Segurança da Informação e Defesa Cibernética

Nome: Edimar Lisboa das Chagas - Suplente. Unidade: CSID - Coordenadoria de Segurança da Informação e Defesa Cibernética

Fiscais administrativos:

Nome: Francisco Carlos Alves Diniz - Titular: Seção de Gestão de Contratações de TIC

Nome: Vanderlei Barbosa da Silva - Suplente: Seção de Gestão de Contratações de TIC

Gestores: Os gestores são definidos pela Coordenadoria de Planejamento e Gestão de Contratos de TIC

Se houver necessidade de designação de comissão de recebimento definitivo, indicar os servidores que serão designados:

(x) A equipe de gestão da contratação contará com servidores que atuarão no seu planejamento, uma vez que estes terão melhor conhecimento das regras e procedimentos suficientes para indicar equipes distintas.

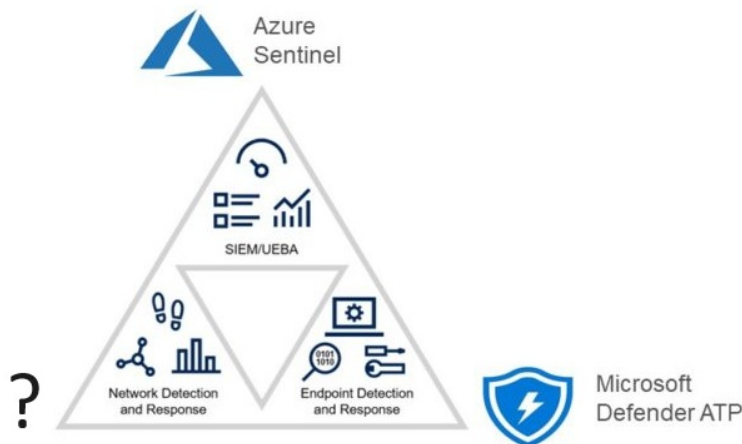
Observação:

2. Necessidade da contratação

2.1 Descrição da Necessidade:

O problema a ser resolvido por esse projeto diz respeito à incapacidade da STI em identificar ameaças diretamente no tráfego de rede, dependendo necessariamente de equipamentos de borda, que analisam o tráfego de forma intrusiva, ou seja participando diretamente da comunicação. Essas soluções são denominadas de NDR (Network Detection and Response) ou NPB (Network Packet Broker - NPB), sendo que esta última realiza a cópia ou recebe espelhamento do tráfego, trata e posteriormente encaminha para o SIEM (Sentinel), conforme o item 4.4.

Com a implementação na infraestrutura de TI do STJ da solução de NDR, a tríade de segurança recomendada pelo Gartner, composta por SIEM (Sentinel), EDR (Endpoint Detection and Response) e NDR (Network Detection and Response), é formada.



3. Requisitos da contratação

3.1 Requisitos legais da contratação:

- (x) Não há conhecimento de nenhuma legislação que exija critérios especiais para contratação do objeto.
- () Aplicação de margem de preferência. Informar a legislação: _____
- () Outras legislações afetas ao objeto a ser contratado: _____

3.2 Apresentação de certidão e/ou atestado:

- () Não há necessidade de apresentação de certidão e/ou atestado.
- (x) Sim. Quais?
- Atestado de capacidade técnica que demonstre que a licitante é capaz de fornecer e implantar de solução de NDR e NPB, de características técnicas sem meses.
 - Comprovação de que a licitante faz parte da lista de parceiros do fabricante da(s) solução(ões) por ela ofertada(s).

Justificativa:

- Tendo em vista o tamanho e complexidade da rede do STJ, bem como a importância desta Corte Superior para o regular funcionamento do Estado Brasileiro, a contratação de uma solução de NDR e NPB, de características técnicas compatíveis com o CONTRATANTE.
- Quanto à exigência de que a licitante seja parceiro do fabricante, visa atender a uma prática do mercado de TI onde somente o parceiro fornece serviços com o respaldo do fabricante. Caso a solução venha a ser adquirida de uma empresa não parceira do fabricante, o STJ poderá não obter o serviço de suporte adequado em caso de problema durante a garantia.

3.3 Exigência de garantia contratual:

- () Não. (x) Sim.

Justificativa: A exigência de garantia contratual se justifica nos termos do art. 139, inciso III, alínea "a", da Lei n. 14.133/2021, ou seja, para eventual pagamento de indenização por danos materiais.

3.4 Requisitos de acessibilidade para equipamentos e acessórios de TIC:

- (x) Não há requisitos de acessibilidade.
- () Sim. Quais? _____

Justificativa:

3.5 Deslocamento de técnico ou disponibilidade em unidade de prestação de serviço local para serviços de manutenção e assistência técnica:

- (x) Não se aplica.
- () Especificação da garantia exigida e das condições de manutenção e assistência técnica acompanhada da justificativa: _____

3.6 Demais requisitos da contratação:

(x) Necessidade de vistoria. **Justificativa:** Considerando a complexidade da solução e a necessidade de interação e integração com diversos ativos de TI já i uma melhor compreensão do ambiente de TI onde a solução será instalada.

(x) Foram avaliadas as diretrizes previstas no art. 11 da [IN STJ/GDG n. 4/2023](#) para a elaboração deste ETP.

() Exigência de carta de solidariedade do fabricante. **Justificativa:** _____

() Exigência de prova de conceito. **Justificativa:** _____

(x) Não serão indicadas regras externas de fabricantes, fornecedores ou prestadores de serviços que possam acarretar alteração unilateral do contrato por pa

() Foi identificado, na base de dados da Plataforma de Governança Digital Colaborativa do Poder Judiciário (Connect-Jus), objeto similar à contratação prete

(x) Aplicação do Guia de Contratações de TI da [Resolução CNJ n. 468/2022](#).

Haverá pagamento antecipado?

(x) Não - REGRA

() Sim. **Justificativa:** _____

4. Soluções de Tecnologia da Informação

4.1 Diferentes soluções de TIC que, com base em levantamento de mercado, possam atender à necessidade do Tribunal*:

A equipe técnica de contratação entende que apenas soluções específicas de NDR e NPB são capazes de atender à necessidade do Tribunal no que tan conceitos e não produtos específicos e apenas soluções que implementam esses conceitos podem então atender os objetivos esperados e especificados nest

Entre os fabricantes que oferecem soluções e produtos que implementam essas funções do NDR e NPB podemos citar, Gigamon, NetScout, Vectra, Fortinet, (

Nesta data, não é de conhecimento dessa equipe técnica da existência de soluções livres, de uso corporativo, que atendam às especificações uma vez que não seria obtido de forma gratuita. O software embarcado também é altamente especializado e complexo, requer atualizações constantes que são feitas por na sua construção e atualização além de integrações com outros fabricantes e compartilhamento de inteligência de segurança entre estes, o que dificulta a exi

O caminho da contratação por meio de licitação, adotando modelo de pregão eletrônico para aquisição de soluções desse tipo foi adotado Tribunal de Contas Catarina (PE n. 102/2021), Defensoria Pública do Estado do Pará, e mais recentemente pelo CJF e, ainda em andamento, pelo TJDF e TRE.

Podem ser avaliados, contudo, modelos de implementação entre os quais identificamos:

a) Implementação de Network Defense and Response sem Network Packet Broker:

Nesse cenário é dispensado toda a infraestrutura de captura de tráfego de rede. Os próprios ativos monitorados são configurados (se suportarem) para espelh

Vantagens

a) Menor custo por dispensar toda a infraestrutura de captura. Entretanto, a inexistência de uma camada própria de captura pode aumentar o custo da solução

b) Menos complexidade de implementação uma vez que envolve um número menor de alterações físicas no ambiente;

Desvantagens:

a) O próprio ativo que será monitorado precisa encaminhar uma cópia do seu tráfego para o NPB, com isso, há um aumento no uso dos seus recursos com equipamento;

b) A configuração é realizada em cada ativo aumentando as possibilidades de falhas, necessidade de reconfigurações.

c) Alguns equipamentos podem não suportar o envio de tráfego de rede, impedindo seu monitoramento;

d) São perdidas todas as funcionalidades de uma solução de packet broker como remoção de tráfego duplicado, remoção de dados irrelevantes sob aspecto d

e) Em decorrência do exposto no item "c", a solução de NDR deverá estar preparada para receber um volume maior de tráfego, exigindo equipamentos maiori seja proporcional a redução de ativos;

Conclusão: Entendemos que esse é um cenário adequado para ambientes menores, com poucos ativos sendo monitorados, que envolva uma complexidad diversos pontos de coleta de tráfego.

b) Implementação de Network Defense and Response com Network Packet Broker:

Esse é o modelo considerado mais indicado para o ambiente a ser monitorado. Suas vantagens e desvantagens seguem no sentido inverso ao do modelo ante

Desvantagens:

a) Envolve a instalação de uma camada específica de captura e essa camada possui um custo próprio o que torna o projeto mais caro.

b) Torna a implementação da solução mais complexa, uma vez que será necessária a instalação de equipamentos específicos para a captura do tráfego de rei

Vantagens:

a) Retira dos ativos monitorados a função de encaminhamento do tráfego de rede, realizando a cópia do tráfego diretamente na fibra ou no cabo de rede;

b) Implementa diversas funções de tratamento do tráfego de rede, como remoção de tráfego duplicado, remoção de dados irrelevantes, filtros de ativos, redes

c) Simplifica a função do NDR e, consequentemente, a necessidade de equipamentos mais robustos e caros;

d) Evita que haja sobrecarga de uso de recursos dos ativos monitorados;

Conclusão: Considerando a complexidade do ambiente, apresentado no item 4.4, entendemos que esse é o cenários mais indicado para o STJ. Nesse cená são disponibilizados diversos recursos de tratamento do tráfego e simplifica a implementação da camada de NDR.

Não há possibilidade, para o escopo desse projeto, do uso de NPB sem o NDR, visto que o objetivo final é obter as funcionalidades do NDR, onde o NPB é considerado em outros cenários, como cópia, backup, etc, não atingiria a finalidade desse projeto.

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

Considerando o exposto no item anterior, não conseguimos identificar diversas soluções de TIC para atender ao propósito desse projeto. Apenas variações d no item anterior, diversos fabricantes dispõem de produtos e solução que implementam as funcionalidade desejadas. Essas funcionalidades são agrupadas e Defense and Response. A estratégia dessa equipe de contratação é promover a máxima concorrência entre os fabricantes dessas soluções, uma vez que não

No item 4.7, apresentamos 3 estimativas, para o cenário "b" do item anterior, de fabricantes diferentes, quais sejam: Lumu (Oakmont), Fortinet (Fasthelp fornecedores das soluções Trendmicro, DarkTrace, Trellix também foram contactados e dos quais esperamos também receber estimativas.

4.3 Avaliação das necessidades de adequação do ambiente do Tribunal:

- a) Infraestrutura tecnológica: O Superior Tribunal de Justiça possui 02 (dois) datacenters adequados para instalação dos equipamentos. Esses equipamentos administradores com os mesmos será feita a partir das suas estações, por meio de consoles de administração. Assim, não há necessidade de adequações ne isso, serão utilizados espaços nos racks existentes.
- b) Infraestrutura elétrica: Os datacenters citados no item anterior possuem infraestrutura elétrica adequada e com capacidade para suportar esses novos e anos, equipamentos que consumiam grandes quantidades de energia tem sido substituídos equipamentos mais econômicos e dessa forma, a capacidade do d
- c) Logística de implantação: Caberá à contratada todo processo de implantação, desde a entrega dos equipamentos na sede do STJ à instalação e entreg internos referentes a horários de funcionamento, gestão de mudança, sustentabilidade, gestão de pessoal entre outros.
- d) Espaço físico: Nesse quesito, novamente resgatamos a existência de 02 (dois) datacenters no STJ onde os equipamentos serão instalados, havendo espaç
- e) Mobiliário: Os equipamentos serão instalados em racks apropriados para equipamentos de TI já disponíveis nos datacenters do STJ.
- f) Impacto ambiental: Quanto ao ambiental, essa questão foi analisada no item 4.4.1 referente ao Ciclo de vida do objeto.

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

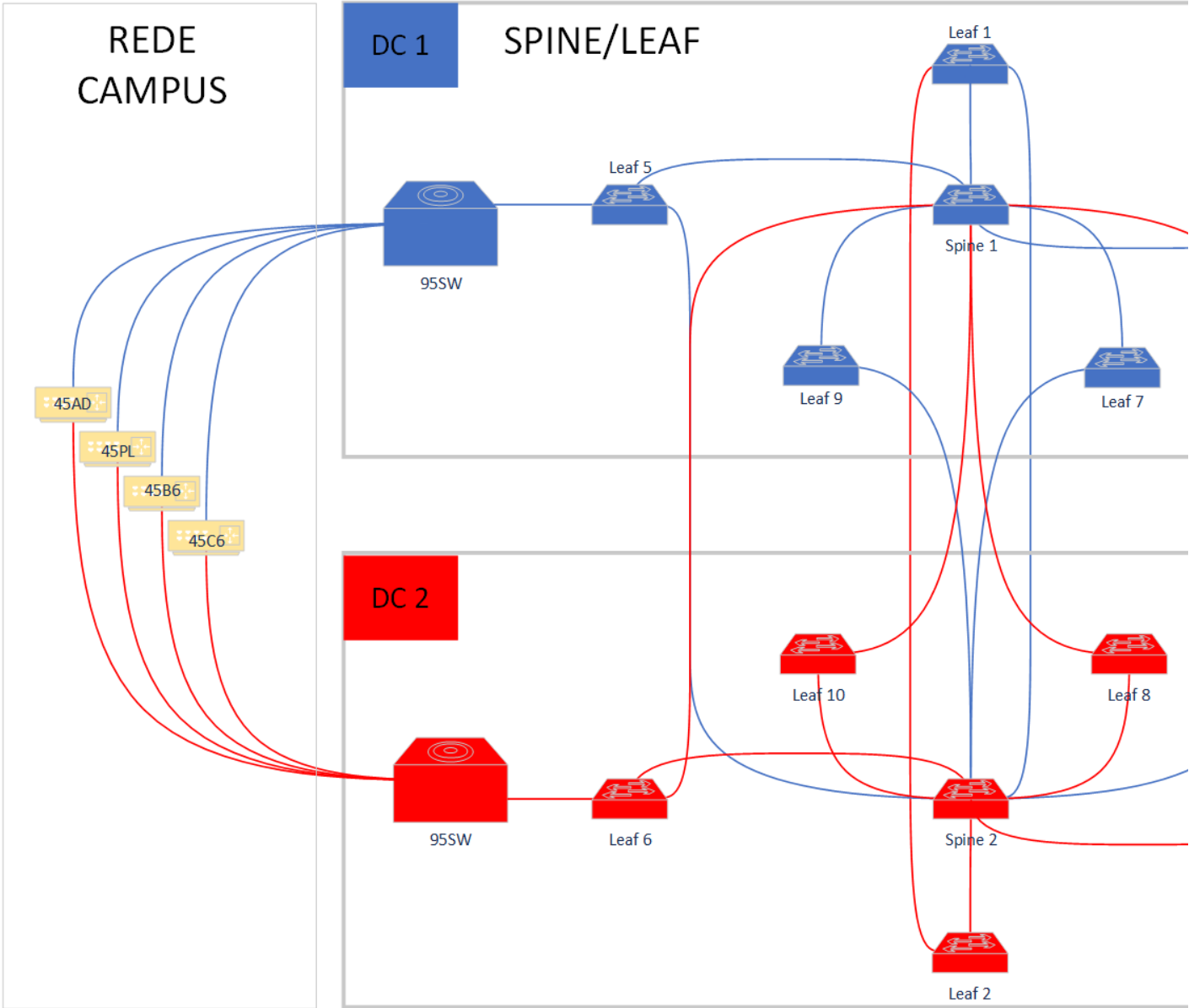
Descrição da Solução:

Trata-se de solução responsável pela captura do tráfego de rede e pela geração de alertas de segurança para equipe de Segurança da Informação do STJ. Esse processo de captura e análise se dá por meio de espelhamento desse tráfego ou encaminhamento direto desse tráfego por outros ativos de TI. Esse tráfego é removido de informações irrelevantes sob o aspecto segurança, anonimização, entre outros, no mercado esse tipo de solução é denominada do Network Pac monitorar e gerenciar continuamente e eficientemente a infraestrutura de rede. Trata-se uma capacidade valiosa na detecção de ameaças, resolução de problemas. Após o tratamento o tráfego resultante é entregue para outra solução especializada em buscas de ameaças a partir do tráfego de rede. Nesse tipo de solução comportamento, bem como técnicas baseadas de assinaturas e, a partir dessas análises, são gerados alertas que por sua vez são encaminhados para ação no mercado como Network Defense and Response.

Assim, a solução descrita é composta por dois elementos:

- a) NDR - Network Detection and Response;
- b) NPB - Network Packet Broker;

O ambiente a ser monitorado está representado na imagem abaixo:



Alinhamento em relação às necessidades de negócio e requisitos tecnológicos

A aquisição está alinhada com Plano Estratégico Institucional referente aos Objetivos Estratégicos de:

- Aprimorar a governança institucional

- Intensificar o uso de tecnologia da informação;

Quanto ao Plano Diretor de Tecnologia da Informação e Comunicação - PDTI 2023 - 2024, essa aquisição está relacionada à aquisição tática "aumentar a maturação das soluções de segurança da SI";

Identificação dos benefícios a serem alcançados com a solução escolhida além dos aspectos de eficácia, eficiência, economicidade e padronização dos objetivos da contratação

O principal objetivo e benefícios a serem alcançados são:

- Ampliação da capacidade da equipe de segurança da informação do STJ de identificar ameaças;
- Permitir uma reação mais precisa e rápida da equipe de segurança da informação do STJ às ameaças identificadas;
- Permitir a automação de respostas às ameaças por meio da aplicação da orquestração de ações pelas demais soluções de segurança;

São objetivos secundários:

- Redução do volume de eventos gerados pelas diversas soluções de segurança;
- Redução do volume de logs gerados diariamente pelas demais soluções de segurança;
- Eventos de segurança com grau de assertividade maior que os obtidos atualmente;
- Redução de custo com armazenamento de grandes volumes de logs que, atualmente são menos efetivos do ponto de vista de geração de alertas de segurança;

Relação entre a demanda prevista e a quantidade dos bens e/ou serviços a serem contratados

A relação entre a demanda prevista e a quantidade está, no entendimento dessa equipe, adequada, uma vez que a solução está sendo adquirida para o cenário

Demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais ou financeiros

Com base no exposto acima, em identificação dos benefícios, podemos deduzir os seguintes resultados:

- Com a redução do volume de logs enviados para soluções de SIEM poderá haver uma redução de custo no armazenamento desses dados.
- Quanto aos recursos humanos, a solução possibilitará uma resposta à ameaças mais rápida e efetiva da equipe operacional;
- Quanto aos recursos materiais, não verificamos possibilidade de impactos significativos, positivos ou negativos;

A possibilidade de aquisição na forma de bens ou contratação como serviço

Qualquer solução de TI pode ser adquirida como serviço e essa é inegavelmente uma tendência, especialmente para serviços em nuvem. Entretanto, para esse caso:

- Todos os ativos monitorados são de propriedade do STJ e estão on-premise (instalados nas dependências do STJ);
- A solução será composta majoritariamente por equipamentos de longa duração, estáveis, cujo uso não sofre ampliações ou reduções constantes, ou sazonalidade de demanda.

Dessa forma, entendemos que a aquisição dos ativos é o melhor cenário para essa solução.

A ampliação ou substituição da solução implantada.

Atualmente o STJ não dispõe de nenhuma solução com as funções e características descritas nesse projeto. O ambiente a ser monitorado está descrito acima

Quanto à ampliação, ou mesmo redução do escopo, tal situação é possível e poderá ocorrer nas seguintes situações:

- Ampliação: Identificação da necessidade de se aumentar a visibilidade do tráfego de rede e análise do tráfego de rede, incluindo outros seguimentos como segurança;
- Redução: Identificação, após o uso da solução, de que certos seguimentos de rede não apresentaram os resultados esperados e dados necessários para a solução;

Quanto à substituição da solução:

- A solução a ser contratada não gerará grande dependência tecnológica e poderá ser substituída se necessário.
- A solução não impacta diretamente o negócio do STJ, de forma que sua descontinuidade ou substituição não provocará interrupções no serviço.
- Durante o processo de substituição da solução, poderá haver uma diminuição da capacidade de resposta a ameaças e a incidentes de segurança o que pode impactar o conhecimento, o aprendizado da equipe técnica que, em uma eventual substituição, exigirá sua reconstrução.

4.4.1 Ciclo de vida do objeto:

Na contratação em comento, cabe fazer as seguintes considerações quanto ao ciclo de vida do objeto:

Fase 1,2,3: Trata-se de produto complexo, cuja cadeia de produção envolve diversos componentes que por sua vez envolvem inúmeras outras cadeias de produção e derivados. Apresenta assim potencial poluidor, que incluem o uso de material de fontes não renováveis, o uso de metais pesados e outras substâncias químicas, etc. Tendo em vista esse potencial poluidor, bem como o risco para a saúde humana do uso de substâncias perigosas, esta prevista a observância de normas que não devem conter chumbo, mercúrio, cádmio, cromo hexavalente, polibromobifenilo (PBB) e/ou éter de difenilo polibromado (PBDE).

Fase 4: Será previsto o acondicionamento dos bens, preferencialmente, em embalagens que utilizem materiais reciclados ou recicláveis.

Fase 5: Quanto ao consumo, por se tratarem de equipamentos eletrônicos voltados para área de tecnologia da informação. Estes consumirão, principalmente o STJ. Esse consumo de energia pode resultar em emissões significativas de gases de efeito estufa, especialmente se a eletricidade for gerada a partir de fonte fóssil. No DataCenter também consome energia, já que é necessário manter as temperaturas dentro dos limites corretos para garantir o funcionamento adequado da infraestrutura. O STJ já possui 02 datacenters ativos, preparados para receber as soluções de TI. O uso adicional de energia por estes equipamentos de tecnologia para topologia. Entretanto, cada dispositivo elétrico dessa solução deve consumir por hora cerca de 500W. Nosso cenário, considerando 2 equipamentos por hora, totaliza 1000W/h.

Fase 6: Os itens a serem adquiridos se enquadram como resíduos de equipamentos elétricos e eletrônicos. Os equipamentos elétricos e eletrônicos possuem vida útil limitada, podem contaminar o solo e os lençóis freáticos, colocando em risco o meio ambiente e a saúde pública. Dessa forma, ao final do ciclo de vida dos equipamentos de tecnologia da informação que, mesmo após o término do contrato e da garantia, podem ainda ser explorados para fins de estudos em escopo de Conduto, é possível o encaminhamento para empresas que realizam a reciclagem desse tipo de material. Vale salientar que o STJ tem parceria com a ON. Quanto à dissipação de calor produzida por esses novos ativos, que deverá ser resfriado pelo sistema de ar-condicionado, ficará em torno de 3000BTU/h por equipamento.

4.5 Sustentação do contrato:

Os recursos materiais e humanos necessários à continuidade do objeto contratado:

O contrato será sustentado pela Coordenadoria de Segurança da Informação e Defesa Cibernética - CSID que possui servidores altamente qualificados para manutenção. Não haverá necessidade de recursos materiais adicionais.

A continuidade do fornecimento da Solução de Tecnologia da Informação e Comunicação em eventual interrupção contratual:

Caso ocorra uma interrupção contratual, a solução será mantida pelos servidores e prestadores de serviços contratados pelo STJ nos contratos de SOC e diretamente do fabricante, não deixando de receber atualizações e poderá, inclusive, ter peças substituídas por este.

Não ficará disponível para o STJ os serviços de suporte técnico do parceiro. O SLA para reposição de equipamentos será prejudicado, uma vez que a reposição é diretamente do fabricante. Assim, nesse cenário, a garantia seguirá os prazos do fabricante e não do contratado.

As atividades de transição contratual e de encerramento do contrato:

Como atividades de transição contratual e de encerramento, devem ser incluídas:

- a) entrega de versões finais dos produtos alvos da contratação;
- b) transferência final de conhecimentos sobre a execução e a manutenção da Solução de Tecnologia da Informação e Comunicação;
- c) devolução de recursos materiais;
- d) revogação de perfis de acesso;
- e) eliminação de caixas postais.

IV – as regras para estratégia de independência do órgão com relação à empresa contratada, que contemplem, no mínimo:

O STJ poderá possuir independência do fornecedor ou fabricante no aspecto de operação da solução o que poderá ser obtido por meio de transferência de conhecimento.

Contudo, dado à alta tecnologia empregada em tais soluções, o uso de hardwares específicos, o uso de informações e dados provenientes de diversas fontes, entre fabricantes, não seria possível o STJ obter independência em relação a esses pontos;

Os produtos gerados pela solução pretendida serão eventos e metadados de segurança referentes aos tráfego de rede do ambiente de TI do STJ. Tais dados são de propriedade do fabricante. Contudo, códigos-fontes das aplicações, modelos de dados e bases de dados, são exclusivos e propriedade intelectual do fabricante, sobre os quais não haverá transferência.

4.6 Estimativa das quantidades a serem contratadas:

Cada fornecedor adota uma forma de licenciamento diferente sendo três as possibilidades:

- Contagem de Dispositivos:
 - Em levantamento realizado no dia 20/03/2024 o número de estações ligadas no STJ era de 3950 e o número de ativos da rede de servidores era de 3.570. Considera-se que esse era o número de equipamentos ligados. Recentemente o STJ adquiriu 3.570 estações por meio do contrato STJ n. 90/2023 e os equipamentos servidores também aumentam de acordo com o surgimento de novos serviços ou para atender ao crescimento natural do uso dos recursos.
 - Um levantamento realizado no Microsoft Azure, também no mesmo dia, informou que nos últimos 3 (três) meses, 5.281 estações haviam se conectado.

Microsoft Azure

Search resources, services, and docs (G+)

Home > STJ- Superior Tribunal de Justiça | Devices > Devices | Overview >

All devices

Download devices

Refresh

Manage view

Enable

Disable

Delete

Manage

Preview features

Got feedback?

Azure Active Directory is now Microsoft Entra ID. Learn More

STJ

Add filters

Enabled: Yes

Join type: Microsoft Entra hybrid joined

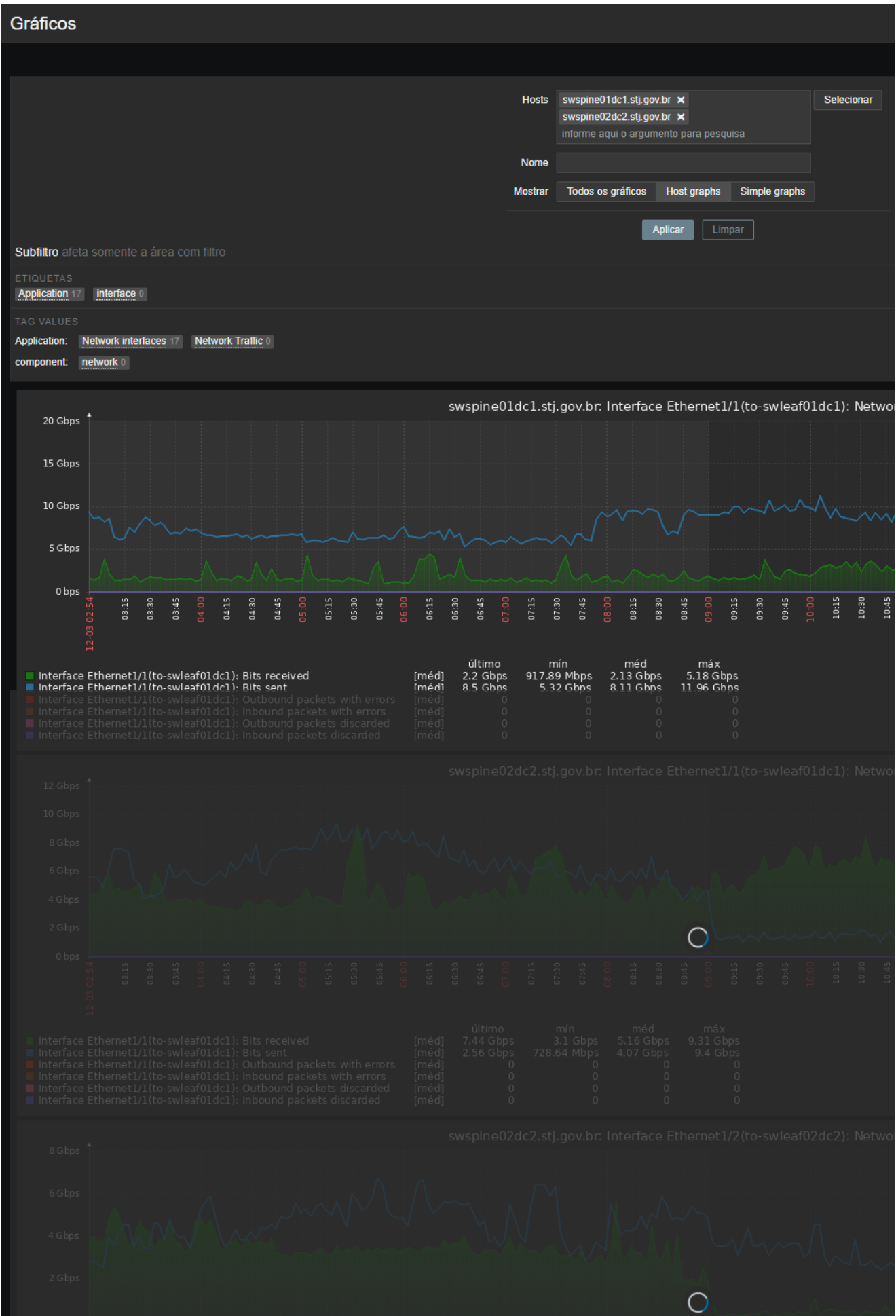
5,281 devices found

	Name	Enabled	OS	Version	Join type	Owner	MDM	Security
	STJ193826	Yes	Windows		Microsoft Entra hybrid joined	None	None	N/A
	stj193854	Yes	Windows	10.0.19045.3930	Microsoft Entra hybrid joined	None	None	N/A
	STJ193900	Yes	Windows	10.0.19045.4046	Microsoft Entra hybrid joined	None	None	N/A

- Como os licenciamentos costumam ser realizados para um número fixo de dispositivos é preciso, geralmente, licenciar um número maior para garantir a continuidade, uma vez que a tendência é aumentar, como por exemplo, pelo retorno do trabalho remoto para presencial.
- Assim quanto à quantidade de dispositivos, consideramos que 5500 licenças deve atender o período de vigência do contrato.
- Contagem de IPs distintos:
 - A contagem de IPs distintos é mais complexa que a de dispositivos. Isso porque um único dispositivo pode ter mais de um IP, já que o IP é atribuído dinamicamente, cada estação de trabalho do STJ possui pelo menos 2, uma para cabeamento físico e outra para rede wireless. Em geral a placa wireless recebe um novo IP a cada intervalo de tempo. Trata-se de uma característica do serviço DHCP que aloca IPs para as estações de acordo com demanda. Se uma estação pode pegar um IP diferente do IP que usava antes. Para o licenciamento, serão dois dispositivos diferentes.
 - Assim, o número de IPs tende a ser maior que o número de dispositivos.
 - Ainda quanto ao licenciamento por número de IPs, é importante considerar que as soluções não levam em consideração somente o que está ativo no momento, mas também o histórico dos últimos 3 (três) meses. Assim, o licenciamento é feito respondendo à seguinte questão: Quantos IPs distintos você tem na sua rede considerando os últimos 3 meses.
 - Assim, considerando o cenário de licenciamento por IP, sugerimos que sejam considerados 7150 mil IPs distintos. Esse número é encontrado pela seguinte fórmula:
- Throughput:
 - Inicialmente podemos definir *throughput* como o volume médio de dados que efetivamente passam pela rede em um período específico. Esse procedimento é feito considerando o histórico de tráfego de rede do STJ nos últimos 3 meses.

que chega das estações de trabalho.

- Será monitorado a rede spine/leaf que concentra toda a comunicação entre os equipamentos servidores do datacenter bem como as requisições e
- A soma do *throughput* de todas as interfaces da rede spine/leaf gera tráfegos médios de 42Gbps conforme resultado da soma dos tráfegos méz ZABBIX. Considerando que o NPB, que enviará o tráfego para o NDR, poderá reduzir esse tráfego, aplicando técnicas de *slicing* (*fatiameto*), em [advanced-flow-slicing.pdf](#) ([gigamon.com](#)) , chegamos a um valor de 20Gbps para o NDR.











Finalizadas essas explicações, consideramos que a solução deverá ser licenciada para até 5500 mil dispositivos, 7150 IPs distintos, 50 Gbps de *throughput* Defense and Response.

4.7 Estimativa do valor da contratação:

No momento da realização desses estudos técnicos preliminares, foram levantados os seguintes preços públicos e propostas comerciais listadas abaixo.

Cabe informar que, no caso dos preços públicos, não foi possível encontrar um projeto que se encaixasse precisamente na nossa especificação. Isso monitoramento específico do datacenter do STJ e possível presumir que, ainda que possa haver alguma semelhança em outros locais, as diferenças como número de datacenters onde serão instalados os dispositivos, volume de tráfego de rede do ambiente monitorado, interferem substancialmente no preço.

Ainda assim, entendemos que os preços públicos listados abaixo podem ser usados para obter uma custo mais aproximado do valor que será obtido em um: um sobrepreço necessário para uma eventual disposta em um pregão.

Preços Públicos

Ata de Registro de Preços n. 016/2022 - DPE/PA (4071040)
Pregão Eletrônico SRP n. 029/2022-DPE/PA
Contratante: Defensoria Pública do Estado do Pará
Prazo: 36 meses
Itens: 03, 04, 05, 06, 15, 16, 18, 19, 20
Valor: R\$ 5.169.390,64
Valor ajustado (regra de 3) para 24 meses: R\$ 3.446.260,42
Corrigido pela SELIC usando Calculadora do Banco Central: **R\$ 4.122.871,49**
Obs: O item 19 dessa ARP possui capacidade inferior ao exigido na especificação do STJ. Um equipamento para o STJ possivelmente terá valor maior.

Pregão Eletrônico n. 102/2021 (4071458)
Contratante: Poder Judiciário do Estado de Santa Catarina - UASG: 925045
Prazo: 60 meses
Valor: R\$ 4.050.000,00 (item 1) + R\$ 2.325.000,00 (item 2) = R\$ 6.375.000,00
Valor ajustado (regra de 3) para 24 meses: R\$ 2.550.000,00
Corrigido pela SELIC usando Calculadora do Banco Central: **R\$ 3.379.168,90**

Propostas Comerciais

Empresa: Oakmont - Documento: 4070845

Item	Descrição	Valor Unitário	Valor Total
1	Network Detection and Response- NDR	R\$ 3.312.899,82	R\$ 3.312.899,82
2	Network Packet Broker - NPB	R\$ 4.354.200,59	R\$ 4.354.200,59
3	Suporte Técnico 24 x 7	R\$ 70.727,02	R\$ 1.697.448,48
4	Instalação e Configuração da Solução	R\$ 497.967,52	R\$ 497.967,52
5	Treinamento para 06 (seis) pessoas	R\$ 43.470,04	R\$ 260.820,24
///	////////////////////////////////	Total	R\$ 10.123.336,65

Obs: Foi verificado que alguns valores totais na proposta não correspondiam aos valores unitários multiplicados pelas quantidades. Devido a isso, foram feitos

Empresa: Fasthelp - Documento: 4070847

Item	Descrição	Valor Unitário	Valor Total
1	Network Detection and Response- NDR	R\$ 23.311.947,70	R\$ 23.311.947,70
2	Network Packet Broker - NPB	R\$ 3.031.619,93	R\$ 3.031.619,93
3	Suporte Técnico 24 x 7	R\$ 32.546,00	R\$ 781.104,00
4	Instalação e Configuração da Solução	R\$ 290.257,35	R\$ 290.257,35
5	Treinamento para 06 (seis) pessoas	R\$ 10.347,75	R\$ 62.086,50
///	////////////////////////////////	Total	R\$ 27.477.015,48

Obs: Foi verificado que alguns valores totais na proposta não correspondiam aos valores unitários multiplicados pelas quantidades. Devido a isso, foram feitos

Empresa: NTSEC - Documento: 4072722

Item	Descrição	Valor Unitário	Valor Total
1	Network Detection and Response- NDR	R\$ 7.991.159,88	R\$ 7.991.159,88
2	Network Packet Broker - NPB	R\$ 7.778.019,62	R\$ 7.778.019,62
3	Suporte Técnico 24 x 7	R\$ 30.660,22	R\$ 735.845,28
4	Instalação e Configuração da Solução	R\$ 582.013,81	R\$ 582.013,81
5	Treinamento para 06 (seis) pessoas	R\$ 10.347,75	R\$ 381.300,60
///	////////////////////////////////	Total	R\$ 17.468.339,19

Valor Estimado

PROPOSTAS COMERCIAIS					
Item	Descrição	Valor Unitário Oakmont	Valor Unitário Fasthelp	Valor Unitário NTSEC	
1	Network Detection and Response- NDR	R\$ 3.312.899,82	R\$ 23.311.947,70	R\$ 7.991.159,88	
2	Network Packet Broker - NPB	R\$ 4.354.200,59	R\$ 3.031.619,93	R\$ 7.778.019,62	
3	Suporte Técnico 24 x 7	R\$ 70.727,02	R\$ 32.546,00	R\$ 30.660,22	
4	Instalação e Configuração da Solução	R\$ 497.967,52	R\$ 290.257,35	R\$ 582.013,81	
5	Treinamento para 06 (seis) pessoas	R\$ 43.470,04	R\$ 10.347,75	R\$ 63.550,10	

PREÇOS PÚBLICOS					
UASG	Órgão	Data	Itens		

	Defensoria Pública do Pará	08/11/2022		
925045	Poder Judiciário do Estado de Santa Catarina	11/11/2021		

Observações:

- a) O valor para o item 1 da empresa FASTHELP foi desconsiderado em virtude do valor elevado em relação aos outros valores obtidos.
- b) O valor médio considerando as propostas recebidas ficou em R\$ 12.469.591,16
- c) O valor médio considerando as propostas recebidas e os preços públicos ficou em: $(R\$ 12.469.591,16 + R\$ 3.751.020,20) / 2 = \text{R\$ } 9.372.727,16$.
- 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 o item).**
- () A licitação pode ser destinada exclusivamente às 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 para 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 na contratação de 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 ou () MAIOR DESCONTO).
- () 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 ou () MAIOR DESCONTO).
- (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 POR ITEM ou () MAIOR DESCONTO).

Justificativa:
Trata-se de uma única solução composta de 02 (dois) itens que envolvem fornecimento de equipamentos e demais itens de serviço, quais sejam, instalação e manutenção, não seria razoável exigir que um fornecedor vendesse outros instalasse outro treinasse e por fim que outro desse suporte, ou qualquer combinação de vinculação entre quem vende e quem presta os serviços e suporte. Além disso, uma divisão nesse nível poderia comprometer seriamente a qualidade do projeto e a dificuldade na atribuição de responsabilidades. Soma-se a isso a existência de diversos contratos administrativos a serem gerenciados que, por si só já geraria uma gestão contratual, dado a necessidade de atendimento a diversas regulações, tornou-se muito mais complexa nos últimos anos;

Quanto aos 02 (dois) itens referentes ao fornecimento de equipamentos, conforme demonstrado em outros documentos, existe uma forte necessidade de suporte secundário sem que as duas soluções trabalhem corretamente. E não se trata somente disso. O desempenho, a qualidade das informações obtidas da solução, a identificação do elemento ou dos elementos responsáveis envolveriam dois fornecedores.

Do ponto de vista administrativo, seriam dois contratos com serviço de treinamento, instalação e configuração e suporte independentes, o que, provavelmente, por fim, o único fornecedor para toda a solução, possibilitará ao fornecedor maior flexibilidade para trabalhar sua planilha de custo, podendo aproveitar seus prazos e reverter-se em benefício para o STJ em uma licitação.

4.9 Contratações correlatas e/ou interdependentes:

Não foram identificadas contratações correlatas ou interdependentes.

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 PCAq no item **STI2024-093** da planilha (4035704).

4.11 Alinhamento entre a contratação e outros instrumentos de planejamento institucional:

Verificar no Documento de Oficialização da Demanda: 3960086

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.
- () bens e serviços especiais: aqueles que, por sua alta heterogeneidade ou complexidade, não podem ser considerados bens e serviços comuns. **Justificativa:**

Tipo de bem (apenas para serviço com fornecimento de bens de consumo):

- (x) O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme art. 2º, II e III, do [Decreto n. 10.818, de 27 de setembro de 2021](#), e a
- () O objeto desta contratação se enquadra como sendo de bem de luxo, conforme art. 2º, I, do [Decreto n. 10.818, de 27 de setembro de 2021](#), e art. 22, I, do

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. 10 de 28 de abril de 2022](#).
- () 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 justificado.
- () O objeto é caracterizado como serviço não contínuo ou contratado por escopo, aquele que impõe ao contratado o dever de realizar a prestação de um serviço 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 junção de esforços de segmentos distintos destinados à sua prestação. Trata-se de serviços comumente prestados por diversas empresas.
- () 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:

- Ampliação da capacidade da equipe de segurança da informação do STJ de identificar ameaças;
- Permitir uma reação mais precisa e rápida da equipe de segurança da informação do STJ às ameaças identificadas;
- Permitir a automação de respostas às ameaças por meio da aplicação da orquestração de ações pelas demais soluções de segurança;
- Redução do volume de eventos gerados pelas diversas soluções de segurança;
- Redução do volume de logs gerados diariamente pelas demais soluções de segurança;
- Eventos de segurança com grau de assertividade maior que os obtidos atualmente;
- Redução de custo com armazenamento de grandes volumes de logs que, atualmente são menos efetivos do ponto de vista de geração de alertas de segu

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

Não identificamos providências adicionais a serem adotadas pela Administração para início da execução do objeto, além das comumente adotadas em qualqu

5.3 Possíveis impactos ambientais:

I – Critérios:

5.3.1 A fabricante e/ou distribuidora, e/ou importadora, e/ou comerciante e/ou consumidora deste objeto deve possuir Cadastro Técnico Federal de Atividades

a) () Sim. A fabricante, e/ou distribuidora, e/ou importadora, e/ou comerciante, e/ou consumidora deste objeto se enquadra nas FTEs do CTF/APP.

b) (x) Não. A fabricante, e/ou distribuidora, e/ou importadora, e/ou comerciante, e/ou consumidora deste objeto não se enquadra nas FTEs do CTF/APP.

5.3.2 A escolha foi por produtos/objetos constituídos de material (marque quantos itens forem necessários):

() renovável () reciclado () atóxico () biodegradável (x) outros: Os produtos que serão fornecidos possuem materiais diversos não sendo passíveis reciclados, atóxicos, tóxicos, biodegradáveis.

() não se aplica

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

() Etiqueta Nacional de Conservação de Energia

() Selo Ruído

() Comprovação de origem de produto de origem florestal (ex: Selo FSC ou Selo CERFLOR)

() Documento de Origem Florestal (DOF) - Transporte e armazenamento

() Ficha de Informações de Segurança de Produtos Químicos (FISPQ)

() Autorização de Funcionamento de Empresa (AFE)

() Requisitos de Avaliação de Conformidade (RAC) para bens de informática - [Portaria INMETRO n. 170/2012](#)

() Diretiva RoHS

() Autorização para o Exercício da Atividade de Revenda de GLP

() Outro(s). Especificar: _____

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

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

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

(x) geração de resíduo: Papelão, plástico, isopor, utilizados na embalagem dos equipamentos. Os equipamentos, em funcionamento, geram calor, que será re

() consumo de papel.

() consumo de outros materiais de expediente (caneta, grampos, clips, pastas etc).

() consumo de café ou açúcar.

() consumo de água mineral envasada.

() instalação de computador ou impressora.

() aparelho de telefone fixo ou móvel.

(x) consumo de energia elétrica: Os equipamentos, em funcionamento, consomem energia elétrica, conforme detalhado no ciclo de vida do objeto.

() 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.

() aumento na 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.

() 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 e da análise realizada pela AGS, caso confirmado impacto eventual inclusão no respectivo plano de ação.

III – Resíduos:

5.3.5 Gestão de resíduos

a) Há previsão de geração de resíduos?

(Observar todos os resíduos gerados pela aquisição e/ou contratação: embalagens, resíduos de instalação, dentre outros, inclusive quanto aos objetos no final

(x) Sim. () Não.

b) Se sim, a destinação ambientalmente adequada dos resíduos será de responsabilidade:

(x) da CONTRATADA (x) do STJ

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

A empresa CONTRATADA deverá se responsabilizar pelo recolhimento e destinação adequada dos resíduos decorrentes da contratação, incluindo e comprometendo-se a declarar ou comprovar, sempre que solicitado pelo CONTRATANTE, os procedimentos adotados para a adequada gestão desses re

c) Descreva os resíduos que serão produzidos - sua natureza, se são classificados como resíduos perigosos (item 3 do Plano de Gestão de Resí

d) Você identifica outros impactos ambientais, além dos indicados acima? (art. 7º, inciso XII, [IN ME n. 40/2020](#)):

(x) Não. () Sim.

Descreva: _____

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?

(x) Não. () Sim. Justificar:

Tendo em vista as características únicas e específicas do ambiente a ser monitorado, entendemos que não há ata de registro de preços que se enquadre perfeitamente.

6.2 Previsão de recursos para a demanda:

(x) A contratação foi prevista na Proposta Orçamentária de 2024, na Ação: STI2024-093.000.

() Não houve previsão orçamentária para contratação.

6.3 Declaração de viabilidade:

Considerando o exposto, declaramos a viabilidade deste processo de contratação.

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:

(x) As informações contidas no presente Estudos Técnico Preliminar **DEVERÃO SER PÚBLICAS, estando disponíveis** para qualquer interessado, pois não

() As informações que não tenham caráter sigiloso serão disponibilizadas na plataforma de Governança Digital Colaborativa do Poder Judiciário (Connect-Ju

() As informações contidas nos itens _____ do presente Estudo Técnico Preliminar **ASSUMEM CARÁTER SIGILOSO**, nos termos do art. 23 da [L](#)

() As informações contidas no presente Estudo Técnico Preliminar **ASSUMEM CARÁTER SIGILOSO**, nos termos do art. 23 da [Lei n. 12.527/2011](#), e, porta

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 pr



Documento assinado eletronicamente por **Uriel Kádmo Nunes Torres, Chefe da Seção de Gestão de Acesso e Eventos de Segurança**, em 19/04/2024, às 12:53, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Leandro Gabriel Bastos Ferreira, Coordenador de Segurança da Informação e Defesa Cibernética**, em 19/04/2024, às 14:10, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Francisco Carlos Alves Diniz, Chefe da Seção de Gestão de Contratações de TIC**, em 20/04/2024, às 12:50, 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 **4076286** e o código CRC **F0239C62**.