Governo do Estado do Rio de Janeiro
Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro
Vice-Presidência de Tecnologia

ESTUDO TÉCNICO PRELIMINAR

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1. Com base nos registros constantes no Estudo Técnico Preliminar cujo objetivo foi identificar e analisar os cenários para o atendimento do Documento de Oficialização da Demanda (100778606), bem como demonstrar a viabilidade técnica e econômica da solução identificada, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação, em consonância com a Lei 14.133/2021, Decreto Estadual 48.816/2023, e os demais normativos vigentes.

1.2. Para consecução da pretensa contratação, ressalta-se que o PRODERJ, autarquia vinculada à Secretaria de Estado de Transformação Digital, atua como Órgão Gestor da Tecnologia da Informação e Comunicação, no âmbito do Governo do Estado do Rio de Janeiro. É responsável por sediar, manter e operar a TIC do Estado, ou seja, os sistemas de informações, o desenvolvimento de sistemas, as bases de dados de vários Órgãos estaduais e os diversos equipamentos hospedados no Data Center do Estado. É responsável também por prover serviços de Internet aos Órgãos da administração estadual, tais como correio eletrônico, consultoria, desenvolvimento e hospedagens de páginas, portais, intranets e extranets.

1.3. Em virtude da meta conduzida pela Secretaria Estadual de Transformação Digital - SETD para a plena digitalização dos serviços, com gradual extinção do “atendimento de balcão”, até o final de 2025, na forma do Decreto Estadual nº 48.671/2023, bem como o avanço do estado nas parcerias com os municípios, promovendo também o processo de transformação digital nas cidades, com apoio tecnológico do PRODERJ, que já levou o sistema de processo eletrônico para 3 (três) municípios e com previsão de chegar em mais 50 cidades, faz-se necessário a adoção de novas tecnologias de proteção e otimização dos ambientes de aplicações, tendo em vista que aumenta exponencialmente os níveis de acessos de usuários, bem como de acessos maliciosos, pois normalmente os criminosos cibernéticos optam por direcionar seus ataques a sistema de prefeituras, que possuem estruturas menores e muitas vezes sem as devidas ferramentas de proteção. No caso em específico desta projeto, o PRODERJ, através da Secretaria de Transformação Digital está hospedando serviços de municípios, o que tende a trazer pras redes corporativas do estado um maior nível de ameaças cibernéticas.

1.4. Na forma do §6º, Art. 1 do Decreto nº 48.209/2022 (atualizado pelo Decreto nº 48.752/2023), cabe ao PRODERJ ***"o fornecimento da infraestrutura tecnológica e dos serviços de tecnologia da informação necessários ao adequado funcionamento do SEI-RJ, inclusive hospedagem, armazenamento, sustentação, segurança da informação, entre outros.".*** Responsabilidade esta que se estende ao SEI-RJ dos municípios.

1.5. Ademais, na forma do Art. 7º do acima citado Decreto nº 48.671/2023, cabe ao PRODERJ a manutenção do Portal Único RJ Digital, com a unificação de informações e serviços prestados pelos órgãos e entidades do Poder Executivo do Estado do Rio de Janeiro.

1.6. Diante dessas atribuições é fundamental que o PRODERJ mantenha os níveis de segurança compatíveis com o papel que desempenha, bem como tenha condições de controlar e dar eficiência ao aumento esperado de tráfego diante das novas responsabilidades..

1.7. Para evitar invasões e sequestro de dados e informações de extrema relevância, o PRODERJ vem buscando mecanismos de inspeção, detecção e bloqueio de ameaças de forma automatizada, proativa e segura.

1.8. A visibilidade total da rede é fundamental para a segurança, especialmente no contexto do conceito Zero Trust (Confiança Zero), que prega que nada na rede é inerentemente confiável. Proteger o que não se vê é impossível, e desafios modernos como a criptografia de dados (TLS 1.3), o aumento da virtualização e o uso de contêineres complicam essa visibilidade.

1.9. O crescimento da virtualização cria uma superfície de monitoramento maior e torna o tráfego Leste-Oeste (entre máquinas no mesmo host) invisível para ferramentas tradicionais. Da mesma forma, o uso extensivo de contêineres introduz novos padrões que exigem ferramentas específicas para monitorar tanto o tráfego Leste-Oeste quanto o Norte-Sul (entrada e saída da rede).

1.10. Para resolver essa falta de visibilidade, é crucial que 100% do tráfego seja inspecionado e analisado por diversas soluções de segurança (firewalls, IPS, anti-malware, etc.). Uma solução de interceptação de tráfego atua como uma camada central, encaminhando somente o tráfego relevante para cada ferramenta de segurança, otimizando o processamento assim como a qualidade da conectividade de rede de modo geral.

1.11. Atualmente, o PRODERJ utiliza múltiplas ferramentas de cibersegurança e observabilidade que tentam processar todo o tráfego da rede de forma ineficiente. Essa não otimização é crítica, pois qualquer atraso na validação do tráfego pode impactar toda a infraestrutura de TIC. A solução de interceptação de tráfego visa otimizar e ampliar o escopo da Segurança da Informação, garantindo que o PRODERJ

consiga ver e analisar tudo o que acontece em sua rede de forma eficaz, proporcionando maior controle e robustez à sua postura de segurança.

1.12. Um dos modos mais eficazes de antecipar às ameaças cibernéticas é através da solução de Network Detection and Response ou mais conhecido como NDR, que possui as seguintes características básicas:

- **Detecção de Atividades Anômalas**:
  - As soluções NDR são projetadas para monitorar o tráfego de rede e identificar comportamentos anômalos que podem indicar uma violação. Isso permite uma resposta proativa em vez de reativa.
- **Integração com o Ecossistema de Segurança**:
  - A NDR pode se integrar a outras ferramentas de segurança, como SIEM (Security Information and Event Management) e soluções de EDR (Endpoint Detection and Response), proporcionando uma visão unificada da segurança da informação.
- **Visibilidade e Monitoramento Contínuo**:
  - A solução proporciona visibilidade completa do tráfego da rede, permitindo que a equipe de segurança monitore continuamente e identifique potenciais ameaças que poderiam passar despercebidas por outras ferramentas.
- **Conformidade e Regulamentação**:
  - Muitas indústrias estão sujeitas a regulamentações rigorosas de segurança de dados (como LGPD, PCI-DSS). A implementação de uma solução NDR ajuda a garantir que a organização esteja em conformidade com essas normas.
- **Resposta a Incidentes Eficiente**:
  - Com recursos de resposta automatizada, a NDR permite que a equipe de segurança reaja rapidamente a incidentes, minimizando danos e tempo de inatividade.
- **Análise Forense e Investigação**:
  - Em caso de um incidente, a solução NDR oferece ferramentas para realizar análises forenses, permitindo entender a origem do ataque e como ele ocorreu.
- **Economia de Recursos**:
  - A automação de tarefas de monitoramento e resposta pode liberar a equipe de segurança para se concentrar em outras áreas críticas, otimizando o uso de recursos humanos.

1.13. O aumento do tráfego, diante do universo maior de usuários ao qual a Administração Pública estará submetida nos próximos anos, demanda não só atenção especial às ameaças cibernéticas, mas principalmente na otimização de sua estrutura interna de conectividade, de forma que se possa garantir a disponibilidade e a melhor experiência de usuário no acessos aos serviços públicos digitais.

1.14. As soluções de observabilidade, interceptação e otimização de tráfego de rede dão ampla visibilidade ao tráfego de rede, permitindo por exemplo, a criação de filtragem de tráfego, garantindo que apenas os fluxos de dados sejam direcionados para as ferramentas que efetivamente precisam, diminuindo consideravelmente o tráfego interno, contribuindo para a estabilidade e velocidade nos acessos aos sistemas, bem como no funcionamento de ferramentas de gestão de segurança e de redes. Abaixo as principais vantagens deste tipo de solução:

- **Visibilidade Total da Rede**:
  - A solução oferece visibilidade abrangente sobre todo o tráfego da rede, permitindo que as equipes de segurança e operações monitorem, analisem e gerenciem o fluxo de dados de forma eficaz.
- **Filtragem de Dados**:
  - Permite a filtragem avançada de tráfego, enviando apenas dados relevantes para as ferramentas de segurança, como SIEM e IDS/IPS, melhorando a eficiência do processamento e reduzindo a carga de trabalho.
- **Detecção de Ameaças**:
  - Facilita a identificação de ameaças ao permitir que ferramentas de segurança tenham acesso a dados de rede completos, melhorando a capacidade de detectar atividades suspeitas e intrusões.
- **Segurança de Dados Sensíveis**:
  - Ajuda na proteção de dados sensíveis, garantindo que apenas informações autorizadas sejam transmitidas e que o tráfego não autorizado seja bloqueado.
- **Desempenho da Rede**:
  - A interceptação de tráfego pode otimizar o desempenho da rede, ajudando a identificar e resolver problemas de latência e largura de banda, garantindo uma experiência de usuário mais suave.
- **Compliance e Auditoria**:
  - Facilita a conformidade com regulamentações de segurança e privacidade de dados, fornecendo registros detalhados de tráfego e acesso, essenciais para auditorias e investigações.
- **Integração com Ferramentas de Segurança**:
  - A solução pode ser facilmente integrada com outras ferramentas de segurança, permitindo uma abordagem holística na proteção da infraestrutura de TI.
- **Análise Forense e Resposta a Incidentes**:
  - Proporciona dados críticos para análises forenses em caso de incidentes de segurança, permitindo que as equipes compreendam como um ataque ocorreu e quais dados foram afetados.
- **Melhoria Contínua**:
  - Os dados coletados podem ser usados para melhorar continuamente a postura de segurança, permitindo que as equipes identifiquem padrões e tendências ao longo do tempo.

1.15. Estas ferramentas contribuirão para o atendimento da Lei Federal nº 13.709/2018, Lei Geral de Proteção a Dados (LGPD) que intensifica a obrigatoriedade de proteção e privacidade dos dados dos titulares, no nosso caso, os cidadãos, reforçando a necessidade do PRODERJ, Órgão de Tecnologia do Estado, contratar e fornecer aos demais Órgãos da Administração Pública Estadual, uma solução que possa proteger os ativos de TIC contra os diversos tipos de ameaças existentes no mundo cibernético, conforme observa-se no Art. 46 da LGPD, onde consta:

> "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

1.16. Pretende-se também atender uma das determinações do Decreto Estadual 47.278/2020, pelo qual o PRODERJ deverá conduzir e disponibilizar as atas de registro de preços e contratos corporativos para suprir itens relativos à TIC aos Órgãos e entidades do Estado.

1.17. Desta forma a presente demanda consiste no robustecimento da segurança e da capacidade de transporte de dados na rede do parque computacional do PRODERJ e demais órgãos da administração pública, mediante disponibilização de soluções de observabilidade, interceptação e otimização de tráfego, além de detecção e resposta a incidentes de segurança.

1.18. A pretensa contratação é necessária, tendo em vista as características de permanente atualização e renovação do ambiente tecnológico, garantindo a continuidade da execução de atividades técnicas críticas. Somem-se a isso, as iniciativas da SETD para levar a transformação digital aos municípios do estado do RJ, iniciando com a hospedagem do sistema SEI no PRODERJ, que trouxe aumento significativo e com crescimento exponencial do tráfego de rede.

2. RELATO DESCRITIVO ACERCA DE CONTRATAÇÕES ANTERIORES VOLTADAS AO ATENDIMENTO DE NECESSIDADE IDÊNTICA OU SEMELHANTE, CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES A ATUAL

2.1. Não há contratações correlatas ou interdependentes previstas, uma vez que o objeto em tela não compõe, no todo ou em parte, nenhum objeto de contrato ou outras soluções existentes na Autarquia.

3. INSTRUMENTO DE PLANEJAMENTO

3.1. A contratação deste objeto se encontra prevista no plano de contratações anual de 2026, conforme detalhamento a seguir:

a) **ID PCA no PNCP**: 44249860000171-0-000030/2026;

b) **Data de publicação no PNCP**: 01/08/2025;

c) **ID dos itens no PCA**: Vide Tabela do Item 11.

3.2. Alinhamento Estratégico

3.2.1. A contratação deste objeto se encontra prevista no Plano Estratégico e Diretor de Tecnologia da Informação e Comunicação - PEDTIC (110308215, p 34 e 35) do PRODERJ:

- **Objetivo Estratégico 1** - Prover, manter e atualizar a infraestrutura e as Soluções e Serviços de Tecnologia da Informação e Comunicação: Prover continuamente a inovação tecnológica para compor e atualizar a infraestrutura, as Soluções e os Serviços de Tecnologia da Informação e Comunicação, atendendo às crescentes demandas da Autarquia e dos Órgãos do Poder Executivo Estadual, visando o desenvolvimento, manutenção, integração e a padronização da TIC do estado (Alinhamento ao PPA 2024-2027 - Programa: 0493 / Ações: 1293 e 1294);
- **Objetivo Estratégico 2** - Ampliar a capacitação técnica e profissional dos servidores em TIC: Promover a qualificação exponencial dos servidores por meio da capacitação e participação em eventos que desenvolvam e aprimorem suas competências e a gestão do conhecimento em TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ação 1293);
- **Objetivo Estratégico 3** - Aprimorar os Processos de TIC: Promover a melhoria contínua dos processos, métodos e técnicas gerando uma maior efetividade na gestão e no uso dos recursos que fornecem as soluções de TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ação 1294);
- **Objetivo Estratégico 6** - Garantir os padrões de qualidade dos serviços e soluções de TIC: Assegurar que os serviços de TIC prestados pelo PRODERJ atendam seus requisitos mínimos, suprindo as expectativas dos órgãos da Administração Pública Direta e Indireta, de modo que contribuam para a agregação de seus valores institucionais e o cumprimento de seus objetivos estratégicos, potencializando sua capacidade de entrega, reforçando a aptidão em produzir, entregar novas soluções e aprimorar as existentes, assim como, o fornecimento de uma infraestrutura inovadora que garantam que os recursos tecnológicos investidos sejam capazes de preservar e promover a segurança, a privacidade, a disponibilidade e a continuidade dos serviços públicos, reduzindo os riscos inerentes aos serviços de TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ações 1293 e 1294).

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. **Necessidade:**

4.1.2. Robustecimento da segurança e da capacidade de transporte de dados na rede do parque computacional do PRODERJ e demais órgãos da administração pública, mediante disponibilização de soluções de observabilidade, interceptação e otimização de tráfego, além de detecção e resposta a incidentes de segurança.

4.1.3. **Funcionalidades:**

4.1.4. As demais especificações estão descritas no ANEXO I - ESPECIFICAÇÃO TÉCNICA, deste documento.

4.2. Requisitos de Capacitação

4.2.1. A CONTRATADA deverá prestar a devida capacitação, de forma on-line, aos usuários (servidores, técnicos e gestores) indicados pela CONTRATANTE, com metodologia de workshop prático (hands on), de forma a preparar os usuários para a operacionalização do sistema.

4.2.2. O treinamento deverá abordar no mínimo: o uso da ferramenta, instalação, configuração, operação da ferramenta, gerenciamento, resolução de problemas.

4.2.3. A CONTRATADA deverá fornecer apostilas e videoaula contendo o material necessário a capacitação ofertada;

4.2.4. O fornecimento dos materiais didáticos (produção e reprodução) será de responsabilidade da CONTRATADA. O material deverá conter a descrição dos diversos componentes envolvidos na solução e os manuais de usuários para auxiliá- los na utilização do ambiente e realizar a transferência de tecnologia e passagem de informações técnicas.

4.2.5. Para o PRODERJ, o quantitativo de alunos será de 06 (seis), para a realização da capacitação.

4.2.6. As capacitações deverão ser realizadas em dias não intervalados, com exceção dos finais de semana.

4.2.7. A CONTRATADA deverá fornecer certificados de conclusão de capacitação emitidos nos nomes dos colaboradores que o executarem, com no mínimo 75% de presença e participação, cujas cópias deverão ser arquivadas pelo CONTRATANTE para fins de comprovação;

4.2.8. A capacitação deverá ser ministrada, preferencialmente, no decorrer da fase de implementação da solução, a critério do CONTRATANTE e devidamente acordado com a CONTRATADA.

4.2.9. A critério do CONTRATANTE a capacitação poderá ser executada em qualquer fase, desde que esteja na vigência do contrato.

4.2.10. Não será admitida a formação de turmas contendo alunos oriundos de diferentes instituições ou contratos.

4.2.11. Os profissionais responsáveis por ministrar a capacitação deverão conhecer todos os aspectos técnicos e funcionais da solução aqui especificada.

4.2.12. Se durante o processo de capacitação, a critério da CONTRATANTE, verificar-se o aproveitamento insatisfatório de qualquer dos instrutores, tal fato será comunicado à CONTRATADA que deverá providenciar a substituição do instrutor no prazo máximo de 48 (quarenta e oito) horas após a notificação emitida pelos fiscais do contrato.

4.2.13. As capacitações deverão ser gravadas em vídeoaulas e disponibilizadas ao CONTRATANTE.

4.2.14. As demais especificações estão descritas no ANEXO I - ESPECIFICAÇÃO TÉCNICA, deste documento.

4.3. **Requisitos Legais**

4.3.1. **Aplicáveis ao Objeto:**

a) **Lei nº 9.609/1998** - Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.

b) **Lei nº 9.296/1996:** Limita e regulamenta a interceptação de comunicações, exigindo autorização judicial para acesso ao conteúdo.

c) **Lei nº 12.965/2014 (Marco Civil da Internet):** Garante a privacidade e a neutralidade de rede, mas permite a guarda de logs e metadados sob certas condições.

d) **Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018 -** Para garantir que as informações do cliente sejam mantidas confidenciais.

- **Art. 6º (Princípios):** Inclui o princípio da **segurança** (medidas técnicas e administrativas aptas a proteger os dados) e da **prevenção** (adoção de medidas para prevenir ocorrência de danos).
- **Art. 48 (Comunicação de Incidentes):** É o artigo mais direto, pois exige que o controlador (a organização) comunique à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares. A capacidade de detectar, analisar e responder a incidentes é fundamental para cumprir este artigo. O SOC é a estrutura operacional para isso.

4.4. **Requisitos de Manutenção**

4.4.1. As soluções, compostas por **equipamentos e serviços de software**, deverão contemplar:

- fornecimento dos bens de forma definitiva, em conformidade com as especificações do fabricante;
- licenciamento de softwares em sua versão mais atual disponibilizada pelo fabricante;
- serviços de manutenção, atualização e suporte técnico, por 36 (trinta e seis) meses.

4.4.2. Não obstante a operacionalização das soluções seja exercida pela CONTRATANTE, todas as rotinas de manutenção necessárias ao pleno e adequado funcionamento dos sistemas e equipamentos, durante o prazo da garantia de 36 (trinta e seis) meses, serão de responsabilidade da CONTRATADA, não gerando quaisquer ônus adicionais para a CONTRATANTE.

4.4.3. O fornecedor deverá disponibilizar ambiente web, número de telefone e e-mail para abertura e acompanhamento de chamados técnicos relativos a qualquer um dos componentes contratados (equipamentos ou softwares).

4.4.4. A CONTRATADA deverá documentar e notificar por escrito as ocorrências sobre eventuais imperfeições, falhas ou irregularidades constatadas na execução dos serviços ou funcionamento dos equipamentos, discriminando de forma inequívoca o componente afetado.

4.4.5. A identificação e a comunicação de defeitos das soluções deverão ser efetuadas dentro do período de garantia, e a totalidade dos defeitos reportados deverá ser corrigida ou substituída pela CONTRATADA, independentemente do lote ou natureza do item (bem ou serviço).

4.4.6. A assistência técnica corretiva deverá ser prestada sempre que solicitada pela CONTRATANTE, mediante abertura de chamado técnico, observando-se os tempos de resposta e de resolução previstos no Acordo de Nível de Serviço (ANS), proporcionalmente à severidade da ocorrência.

4.4.7. Nos casos em que a resolução de chamados técnicos exija intervenção direta nos ambientes da CONTRATANTE, a intervenção deverá ser precedida de planejamento, com avaliação de riscos e impactos, e sua execução deverá ocorrer preferencialmente fora do horário de produção.

4.4.8. Os atendimentos deverão contar com suporte remoto especializado por analistas certificados nas soluções contratadas, com possibilidade de escalonamento ao fabricante, quando necessário.

4.4.9. A manutenção corretiva deverá ser realizada sempre que houver falhas em funcionalidades, recursos, integrações ou no funcionamento dos equipamentos, incluindo interfaces entre os sistemas, relatórios e regras de negócio. As falhas deverão ser classificadas pelo usuário conforme Gravidade e Urgência, sendo priorizadas segundo a metodologia de avaliação e aceite definida neste documento.

4.5. **Requisitos Temporais**

4.5.1. Se encontram previstos no item **"Prazos e Condições de Entrega dos Bens e Serviços"**.

4.6. **Requisitos de Metodologia de Trabalho**

4.6.1. A equipe a ser disponibilizada pelo fornecedor para prestação de todos os serviços deverá seguir as melhores práticas de mercado para cumprimento das atividades objeto da contratação.

4.6.2. As atividades a serem desenvolvidas pela CONTRATADA possuem os seguintes requisitos:

4.6.3. Deverão ser realizadas respeitando o horário de funcionamento de cada local do CONTRATANTE.

4.6.4. Por demanda do CONTRATANTE, poderão sofrer alterações de cronograma dos serviços, desde que não impliquem custos adicionais para a CONTRATADA.

4.6.5. Durante a vigência do contrato, o CONTRATANTE poderá realizar, conforme seu critério, reuniões técnicas e gerenciais com a CONTRATADA, a fim de analisar as entregas das demandas requisitadas pela Administração, definindo as prioridades e estabelecendo um acordo de esforço e prazo para seu atendimento.

4.6.6. São instrumentos formais de comunicação entre o CONTRATANTE e a CONTRATADA:

a) Ordem de Fornecimento;

b) Ordem de Serviço;

c) Plano de Inserção;

d) Termos de Recebimento;

e) Chamado registrado na Central de Atendimento;

f) Ofícios;

g) Relatórios e Atas de Reunião;

h) E-mail; e

i) Demais Termos previstos no instrumento convocatório.

4.6.7. A comunicação entre o CONTRATANTE e a CONTRATADA, para fins de encaminhamento de Autorização de Fornecimento ou Ordem de Serviço, ocorrerá sempre por intermédio do preposto, ou seu substituto, designado pela CONTRATADA.

4.6.8. A comunicação dos usuários com a Central de Atendimento/Suporte da CONTRATADA poderá ser realizada por meio de abertura de chamado via telefone com registro de protocolo ou utilização de sistema informatizado que permita o registro da demanda.

4.7. **Indicação de marcas (ou modelos) e vedação de utilização de marca**

4.7.1. Maiores detalhamentos e definições acerca da manutenção da marca ou de sua substituição serão evidenciados no presente estudo durante o levantamento de soluções existentes no mercado, que revelará o cenário mais viável do ponto de vista técnico e econômico.

4.8. **Dos Requisitos de Privacidade e Proteção de Dados Pessoais**

4.8.1. **Dados Tratados e de Uso Compartilhado**

4.8.1.1. **Dados Compartilhados**: O tratamento de dados no escopo deste projeto poderá ser utilizados para fins de capacitação, Fluxos de dados; Dados de rede completos; Informações autorizadas e tráfego não autorizado; e Registros detalhados de tráfego e acesso.

4.8.1.2. A execução do projeto segue rigorosamente os princípios da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), garantindo que todos os processos envolvendo dados pessoais sejam conduzidos com transparência, segurança e minimização de riscos.

4.8.1.3. O compartilhamento de dados tem como objetivos garantir o processamento dos dados compartilhados de tráfego e fluxo de rede com o objetivo primordial de fortalecer a segurança cibernética, garantir a conformidade regulatória e otimizar o desempenho da rede; é importante ressaltar que o tratamento dos dados pessoais estará sempre alinhado com a LGPD, garantindo a segurança e a privacidade das informações dos cidadãos.

4.8.2. **Finalidade do Tratamento e Compartilhamento**

4.8.2.1. Os dados poderão ser utilizados para fins de capacitação, Detecção de Atividades Anômalas e Ameaças; Visibilidade e Monitoramento Contínuo; Integração com Ecossistemas de Segurança; Conformidade e Regulamentação; Resposta a Incidentes Eficiente; Análise Forense e Investigação; Otimização de Desempenho da Rede; Filtragem de Dados; Segurança de Dados Sensíveis; Auditoria; e Melhoria Contínua da Postura de Segurança. O compartilhamento desses dados visa assegurar a finalidade legítima e a necessidade de cada informação, com o compromisso de segurança da informação em todas as etapas. O registro em logs será mantido para todas as operações de compartilhamento, visando a auditoria. Todo o tratamento e compartilhamento de dados pessoais estará sempre alinhado com a LGPD, priorizando a segurança e a privacidade das informações dos cidadãos.

4.9. **Requisitos de Sustentabilidade Ambiental**

4.9.1. A contratação não trará impactos ambientais significativos, por se tratar de licenças digitais e equipamentos, não se faz necessário declaração de não ofertar produtos com materiais perigosos.

4.9.2. A CONTRATADA deverá priorizar, para a execução dos contratos, a utilização de bens que sejam – no todo ou em partes – compostos por materiais recicláveis, atóxicos e biodegradáveis.

4.9.3. Para os casos em que a oferta dispor de equipamentos, complementados por seus respectivos licenciamentos, a CONTRATADA deverá comprovar que sua oferta está em conformidade com a diretriz RoHS (Reduction of Hazardous Substances).

4.10. **Requisitos Sociais e Culturais**

4.10.1. Não se aplicam requisitos sociais e culturais para esta contratação.

4.11. **De Arquitetura Tecnológica**

4.11.1. As demais especificações estão descritas no ANEXO I - ESPECIFICAÇÃO TÉCNICA, deste documento.

4.12. ***De Projeto e da Implantação***

4.12.1. As demais especificações estão descritas no ANEXO I - ESPECIFICAÇÃO TÉCNICA, deste documento.

4.13. ***Das atualizações do sistema***

4.13.1. Sempre que houver o lançamento de nova versão do sistema ou correções de segurança que possam comprometer os serviços prestados, o CONTRATANTE deverá ser notificada com antecedência e a atualização do sistema providenciada pela CONTRATADA, sem custos adicionais ou impactos para o CONTRATANTE. Atualizações que não sejam motivadas por erros ou problemas de segurança só poderão ser realizadas das 23:00 às 06:00 nos dias úteis ou nos fins de semana e feriados.

4.14. **Exigência de Credenciamento**

4.14.1. A qualidade de revenda ou distribuidor autorizado é condição indispensável para a entrega do objeto. Isso se dá porquanto os fabricantes restringem a venda e manutenção de seus produtos apenas aos canais devidamente autorizados.

4.14.2. Esta é uma prática extremamente comum no mercado de TI. Através desta exigência, os fabricantes visam assegurar qualidade no serviço de implantação de suas soluções.

4.14.3. Diante das considerações expostas, entende-se que é preciso exigir a apresentação de declaração do fabricante da solução informando que a empresa é autorizada a comercializar licenças e prestar serviços de garantia de atualização e funcionamento dos softwares solicitados.

4.14.4. Demais requisitos estão detalhados no ANEXO I - Especificações Técnicas do Objeto.

4.14.5. A apresentação da Carta de Credenciamento ocorrerá após a homologação e precederá a contratação que estará condicionada à apresentação da carta de credenciamento.

4.14.6. Diante das considerações expostas, entende-se que é preciso exigir o credenciamento da empresa junto ao fabricante, contudo, apenas da empresa vencedora do certame, na etapa que visa a assinatura de instrumento contratual, após a homologação, oriundo da ata de registro de preços, neste feito. A não apresentação da carta de credenciamento implicará a desclassificação da empresa vencedora e será chamada a empresa 2ª colocada no certame, e assim sucessivamente, até que a presente exigência seja efetivamente cumprida.

4.15. **De Garantia / Suporte Técnico**

4.15.1. Define-se nesta documentação o suporte técnico / garantia, o atendimento necessário para os chamados a complementação de configuração, dúvidas técnicas, operacionais e procedimentais para a solução proposta.

4.15.2. A CONTRATADA deverá realizar toda e qualquer configuração na solução, conforme solicitação da CONTRATANTE, seja on-site ou de forma remota, estando obrigada a esclarecer dúvidas técnicas, operacionais, procedimentais, aos usuários da equipe técnica da CONTRATANTE;

4.15.3. A assistência técnica corretiva será realizada sempre que solicitada pela CONTRATANTE por meio de abertura de chamado técnico, acionando diretamente a CONTRATADA;

4.15.4. A resolução de chamados de Suporte Técnico que necessitem de intervenção direta nos ambientes da CONTRATANTE deverá ser precedida de planejamento e somente poderá ser implementada no ambiente, fora do horário de produção e após avaliação do impacto;

4.15.5. Se houver lançamento de uma nova versão de sistema operacional que faça correções de segurança, a CONTRATADA deve informar à CONTRATANTE e proceder a atualização do produto;

4.15.6. O suporte técnico inclui também a validade técnica, conforme definido na Lei Federal nº 9.609/98, no que concerne a possíveis modificações tecnológicas tais como, mas não exclusivamente:

a) Atualizações de versão e correções de erros das soluções de software;

b) Acesso para downloads de patches, drivers, atualização de software e quaisquer outras atualizações de softwares necessárias, que devem estar disponíveis no website do fabricante da solução, sem custos adicionais ao CONTRATANTE, durante todo o período de suporte;

c) Em caso de o software adquirido/contratado ser descontinuado durante o período de vigência contratual, a empresa CONTRATADA deverá fornecer a nova versão do produto equivalente, na mesma quantidade estabelecida em contrato, de modo a garantir a continuidade da solução;

d) Vulnerabilidades (SQL Injection, etc);

e) Sistemas operacionais, servidores de aplicações, etc., sendo tratadas como manutenções eventuais as modificações tecnológicas (por força da Lei 9.609/98); e

f) Disponibilizar as revisões dos manuais técnicos e/ou documentação dos softwares licenciados.

4.15.7. O suporte técnico deverá:

a) Permitir a abertura, acompanhamento e validação de chamados através de e-mail e/ou website (portal do cidadão) e/ou telefone (0800) no regime 24x7x365, com atendimento em português;

b) Possuir canal com os fabricantes envolvidos na solução dos incidentes, bem como ser responsável pela abertura e acompanhamento dos chamados junto aos mesmos;

c) Possuir os processos de gerenciamento de incidentes, requisição, eventos, problemas, mudanças, incidentes críticos e atendimento aos usuários;

d) Suporte técnico de 2º nível quanto a dúvidas de customização e configuração do equipamento e console de gerenciamento.

4.15.8. Na abertura de chamados técnicos serão fornecidas informações pela CONTRATANTE, como:

a) Anormalidade observada;

b) Nome do responsável pela solicitação do chamado técnico;

c) Sistema/versão/módulo/item;

d) Natureza do problema;

e) Descrição da natureza enfrentada.

4.15.9. O atendimento técnico deverá atender os seguintes requisitos técnicos:

a) As solicitações de atendimento de suporte, só poderão ser realizadas pelos contatos cadastrados, em qualquer horário por e-mail e telefone;

b) O atendimento remoto de Suporte e Monitoramento pelos canais: telefônico ou web ou e-mail, funcionará em regime 24 horas por dia, 7 dias por semana para incidentes e solicitações elegíveis de se resolver remotamente;

c) O atendimento presencial de Suporte de incidentes e solicitações elegíveis de se resolver presencialmente funcionará, preferencialmente, no horário comercial das 9:00h às 18:00h. Exceto quando o suporte for emergencial. Nestes casos, o atendimento deverá ser fora do horário comercial em regime 24x7.

4.15.10. A CONTRATADA, após a realização do suporte, deverá apresentar os Relatórios contendo:

a) Identificação do chamado;

b) Data e hora do início e término do atendimento com a solução do chamado técnico;

c) Identificação do defeito;

d) Técnico responsável pela solução do defeito, as providências adotadas, origem do problema e outras informações pertinentes;

e) Atualizações de software/versões realizadas;

f) Acionamentos feitos à equipe da CONTRATADA;

g) Relatórios Extraordinários.

4.15.11. A manutenção corretiva ocorrerá de falha de funcionalidades ou de recursos do sistema, de qualquer natureza, detectada pelo usuário, ou seja, em desacordo com as funcionalidades definidas nas telas, nas regras de negócio, nos relatórios, interfaces com outros sistemas, dentre outras. Tais falhas devem ser classificadas, pelo usuário, observando a GRAVIDADE e a URGÊNCIA e conforme essa definição será feito a priorização, conforme acordo de nível de serviço deste documento.

4.15.12. A CONTRATANTE poderá solicitar, sem qualquer ônus adicional, a substituição ou correção da solução de software, quando se verificarem vícios, defeitos ou incorreções.

4.15.13. Os profissionais deverão fornecer suporte técnico e operacional necessários ao bom funcionamento do sistema, envolvendo os seguintes serviços:

a) Dirimir dúvidas e resolver problemas relativos às características técnicas, funcionamento lógico e físico do sistema.

b) Fazer avaliação e emitir parecer técnico em situações anormais de funcionamento do sistema.

c) Prestar assessoria para adequação do sistema à legislação vigente.

d) Simulações deverão ser efetuadas em paralelo, isto é, mantendo íntegros os dados do cadastro do sistema. A CONTRATADA deverá prover ambiente com cópia integral da base de dados para testes, simulações e homologações para áreas da Contratante, sempre que necessário.

e) Acionar equipe necessária para solução de questões em que os servidores indicados pela Contratante não tenham condições de atender no que diz respeito à operação e configurações do sistema.

4.15.14. O suporte técnico / garantia se configura em aspecto agregado à solução, cujo lapso temporal não se confunde com o lapso de vigência do contrato.

4.15.15. O suporte técnico / garantia deverá ser de 36 (trinta e seis) meses, a contar da emissão do termo de recebimento definitivo, ou do prazo estabelecido pelo fabricante, caso este seja maior.

4.15.16. Alterações na legislação vigente que impliquem manutenções no sistema para sua adaptação ou adequação, desde que não alterem estrutura básica dos sistemas, estão incluídas nessa garantia e devem ser executadas, testadas e homologadas em tempo para assegurar que a CONTRATANTE não perca nenhum prazo legal.

4.16. **De Experiência e Formação da Equipe que Executará os Serviços Relacionados à Solução de TIC**

4.16.1. A equipe a ser disponibilizada pela CONTRATADA para prestação de todos os serviços, deverá ser qualificada e com experiência na atividade objeto da contratação.

4.17. **Requisitos Materiais e Humanos**

4.17.1. Em observação ao entendimento do Enunciado nº 14, item 5 da Procuradoria-Geral do Estado do Rio de Janeiro - PGE/RJ, saliente-se que o objeto da presente contratação não prevê o uso de mão de obra residente nas dependências dos órgãos e entidades CONTRATANTES.

4.17.2. Não será necessária a utilização de mão de obra especializada, tendo em vista que os recursos humanos necessários à instalação e configração da solução, bem como responsáveis pelas manutenções preventivas e corretivas, já fazem parte do escopo do objeto e não será contratado como item específico. Adicionalmente registre-se que o objeto também não caracteriza, de forma alguma, terceirização de atividade-fim, tendo em vista que os serviços serão prestados no âmbito da garantia comum de mercado, que estão diretamente relacionados à atuação de profissionais e especialistas nas soluções contratadas.

4.18. **Necessidades de Adequações no Ambiente**

4.18.1. O CONTRATANTE deverá proceder a todos os ajustes que se mostrarem necessários ao alinhamento e/ou adequação de seus processos internos e outras transições necessárias de modo a assegurar uma satisfatória execução contratual. Tais adequações serão verificadas em vistoria técnica no ambiente do CONTRATANTE, e tratadas em reunião de **kick-off.** A CONTRATADA deverá verificar se o ambiente do CONTRATANTE está adequado para instalação local da solução, em cumprimento aos requisitos estabelecidos pelo fabricante, caso negativo, deverá informar ao CONTRATANTE para que esta possa sanear as pendências antes da execução contratual.

4.18.2. As demais especificações estão descritas no ANEXO I - ESPECIFICAÇÃO TÉCNICA, deste documento.

4.19. **Reunião de kick-off**

4.19.1. As demais especificações estão descritas no ANEXO I - ESPECIFICAÇÃO TÉCNICA, deste documento.

5. LEVANTAMENTO DE MERCADO

5.1. Os estudos elaborados pela Equipe de Planejamento da Contratação visam identificar, analisar e elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

5.2. Para compor esta solução se faz necessário a junção de uma solução de segurança, uma solução de hadware e licenciamento de softwares e uma solução de Gerenciamento e orquestração, baseado nisso, dividimos o estudo em 3 cenários:

5.3. **CENÁRIO 1 - Solução de Segurança, onde fazemos o comparativo entre as soluções:**

5.4. **Solução 1:** Contratação de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação em appliance; **Solução 2** - Contratação de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, baseado em serviço SOC-as-a-Service (Security Operations Center-as-a-Service) e **Solução 3** - Implantação de uma solução de software livre.

5.5. **CENÁRIO 2 - Solução de Infraestrutura de rede Hardware e Software, onde fazemos o comparativo entre as soluções:**

5.5.1. **Solução 1 -** Componentes de Hardware para a captura e o monitoramento de tráfego sem a interceptação do conteúdo e Solução 2 - Componentes de Hardware e Interceptação de Tráfego e Licenciamentos integrados.

5.6. **CENÁRIO 3 - Solução de Gerenciamento e Orquestração, onde fazemos o comparativo entre as soluções:**

5.6.1. **Solução 1 -** Elastic Cloud Enterprise serviços profissionais especializados - ECE e **Solução 2 -** Software splunk enterprise e serviços profissionais especializados

5.7. Dentre as opções disponíveis para atendimento da demanda, foram identificadas e analisadas as seguintes alternativas:

5.8. **CENÁRIO 1 - Solução de Segurança**

5.8.1. **Solução 1**: **Contratação de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação em appliance.**

5.8.1.1. Trata-se de uma solução de segurança robusta que atua diretamente na rede do CONTRATANTE. O objetivo principal é identificar e reagir a atividades incomuns ou maliciosas que possam indicar uma ameaça à segurança da informação.

- **Monitoramento de Comportamento Anômalo da Rede:** Em vez de apenas procurar por ameaças conhecidas (como vírus já catalogados), essa parte da solução observa o **comportamento normal** da sua rede. Se um dispositivo começar a fazer algo atípico — como um computador que nunca acessa servidores de dados começar a enviar grandes volumes de informações para fora da rede, ou um usuário tentar acessar sistemas que não fazem parte de suas permissões habituais —, a solução sinaliza essa anomalia. É como ter um guarda que não só conhece os criminosos procurados, mas também percebe quando alguém está agindo de forma estranha no prédio.
- **Detecção, Análise e Resposta de Incidentes de Segurança da Informação:**
    - **Detecção:** Ao identificar um comportamento anômalo ou uma assinatura de ataque conhecida, a solução gera um alerta.
    - **Análise:** Em seguida, ela coleta e analisa dados detalhados sobre o incidente para entender a natureza da ameaça, sua origem, o que foi comprometido e seu potencial impacto.
    - **Resposta:** Com base na análise, a solução ou a equipe de segurança pode tomar ações imediatas para conter o incidente. Isso pode incluir bloquear tráfego malicioso, isolar dispositivos comprometidos, desativar contas de usuários ou alertar os administradores para intervenção manual. O objetivo é minimizar o dano e restaurar a segurança.
- **Em Appliance:** Isso significa que a solução é entregue como um hardware dedicado (um "aparelho" físico) ou como uma máquina virtual pré-configurada. Ao invés de ser apenas um software que é instalado em qualquer servidor, o appliance é otimizado para a função de segurança, muitas vezes com hardware especializado para alto desempenho na análise de tráfego de rede em tempo real. Isso simplifica a implantação e garante que a solução tenha os recursos necessários para funcionar de forma eficaz.

5.8.1.2. Em resumo, esta solução de NDR (Network Detection and Response) em appliance é essencial para a segurança de rede. Ela atua como um sistema de vigilância inteligente que vai além da detecção de ameaças conhecidas, identificando comportamentos anômalos e incomuns no tráfego da rede. Isso permite a detecção proativa de ataques sofisticados ou inéditos. Após a detecção, a solução analisa profundamente o incidente para entender sua natureza e impacto, e então facilita a resposta rápida e eficaz, seja automaticamente (bloqueando tráfego ou isolando dispositivos) ou alertando administradores. A entrega em appliance garante otimização de desempenho e facilidade de implementação. Desta forma, essa solução capacita a CONTRATANTE com uma defesa cibernética robusta e ágil, protegendo dados e sistemas contra ameaças complexas.

Análise Comparativa (Benchmarking)

- **Darktrace:** https://www.darktrace.com/
- **Vectra AI:** https://www.vectra.ai/
- **ExtraHop:** https://www.extrahop.com/
- **Gatewatcher:**https://www.gatewatcher.com/
- **Cisco:** https://www.cisco.com/
- **ThreatBook:** https://www.threatbook.com/ (Site em chinês, com opção para inglês)
- **Trend Micro:** https://www.trendmicro.com/
- **Stellar Cyber:** https://stellarcyber.ai/
- **Hillstone:** https://www.hillstonenet.com/
- **Corelight:** https://corelight.com/
- **Broadcom:**https://www.broadcom.com/ (Controladora da Symantec Enterprise Security)
- **Sangfor:** https://www.sangfor.com/
- **Fortinet:** https://www.fortinet.com/
- **Lumu:** https://lumu.io/
- **LinkShadow:** https://www.linkshadow.com/
- **NetWitness (parte da RSA):** https://www.netwitness.com/
- **Plixer:** <-block>https://www.plixer.com/
- **Qi An Xin Technology:** https://www.qianxin.com/ (Site em chinês)
- **Exeon:** https://exeon.com/
- **IronNet:** https://www.ironnet.com/
- **Gigamon:** https://www.gigamon.com/
- **Stamus Networks:**https://stamus-networks.com/
- **Sophos:** https://www.sophos.com/

Vantagens:

- Detecção de Ameaças Desconhecidas (Dia Zero): Esta é uma das maiores vantagens. Ao invés de depender apenas de assinaturas de ameaças conhecidas (como antivírus tradicionais), a solução analisa padrões de comportamento na rede. Isso permite identificar atividades maliciosas totalmente novas, para as quais ainda não há defesas catalogadas.
- Visibilidade Abrangente da Rede: Oferece uma visão profunda e em tempo real do que está acontecendo em toda a rede, incluindo tráfego leste-oeste (entre servidores internos) e norte-sul (entrada e saída da rede). Isso revela comunicações suspeitas, movimentos laterais de atacantes e tentativas de exfiltração de dados que outras ferramentas podem não perceber.
- Identificação de Movimentos Laterais e Ataques Internos: É excelente para detectar quando um atacante, após invadir um ponto inicial, tenta se mover por outros sistemas dentro da rede. Também ajuda a identificar comportamentos anômalos de usuários internos que possam indicar ameaças internas (insiders) ou contas comprometidas.
- Resposta Rápida a Incidentes: Ao automatizar a detecção e, em muitos casos, a resposta inicial (como bloquear um IP malicioso ou isolar um dispositivo), a solução reduz significativamente o tempo necessário para conter um ataque, minimizando o impacto.
- Análise Comportamental Avançada (IA/Machine Learning): Utiliza inteligência artificial e aprendizado de máquina para construir um "baseline" do comportamento normal da rede. Desvios desse baseline são rapidamente sinalizados, tornando a detecção mais precisa e eficiente ao longo do tempo.
- Redução da Fadiga de Alertas: Embora possa gerar alertas no início, soluções NDR maduras utilizam análises sofisticadas para correlacionar eventos e priorizar alertas, ajudando as equipes de segurança a focar nas ameaças reais e reduzir o volume de falsos positivos.
- Complemento a Outras Ferramentas de Segurança: Não substitui firewalls ou soluções EDR (Endpoint Detection and Response), mas as complementa. O NDR foca na rede, enquanto o EDR foca nos dispositivos finais. Juntas, elas proporcionam uma defesa em profundidade mais robusta.

- Facilidade de Implantação (em Appliance): O fato de ser entregue em appliance (hardware ou VM pré-configurada) simplifica a instalação e configuração, pois o hardware e software já vêm otimizados para a função.

Desvantagens:

- Custo e Complexidade: Soluções NDR podem exigir um investimento significativo em hardware (para o appliance), software e, muitas vezes, em pessoal especializado para configurá-las, gerenciá-las e analisar os resultados. O custo inicial pode ser elevado.
- Volume de Dados e Armazenamento: Monitorar e armazenar grandes volumes de tráfego de rede requer alta capacidade de armazenamento. O crescimento da rede pode tornar o dimensionamento da solução um desafio e gerar custos adicionais de armazenamento e processamento.
- Falsos Positivos: Embora soluções modernas busquem minimizá-los, a detecção de anomalias pode gerar um certo número de falsos positivos, ou seja, alertar sobre atividades que são incomuns, mas não necessariamente maliciosas. Isso pode sobrecarregar as equipes de segurança se não for bem ajustado.
- Limitação com Tráfego Criptografado: O monitoramento do tráfego criptografado (HTTPS, VPNs) pode ser um desafio. Embora algumas soluções NDR possam integrar-se com proxies de descriptografia SSL/TLS, a visibilidade total do conteúdo criptografado pode ser limitada sem medidas adicionais, o que pode deixar brechas.
- Visibilidade Limitada do Endpoint: A solução NDR foca primariamente no tráfego de rede. Ela pode não ter visibilidade detalhada do que acontece dentro de um endpoint específico (processos, arquivos, registros), sendo necessária a integração com soluções EDR para uma visão completa do incidente.
- Preocupações com Privacidade e Conformidade: O monitoramento contínuo do tráfego de rede pode levantar questões de privacidade, especialmente em ambientes onde dados sensíveis ou pessoais trafegam. É fundamental garantir a conformidade com regulamentações de proteção de dados (como a LGPD no Brasil).
- Saturação em Redes Muito Grandes/Complexas: Em redes extremamente grandes e com tráfego muito intenso, a capacidade de processamento do appliance pode ser testada, levando a gargalos ou à necessidade de múltiplos appliances e uma arquitetura mais complexa.

5.8.2. **Solução 2 - Contratação de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, baseado em serviço SOC-as-a-Service (Security Operations Center-as-a-Service).**

5.8.2.1. Trata-se de uma solução de prestação de serviço de segurança cibernética que opera na nuvem.

- **Monitoramento de Comportamento Anômalo da Rede:** Esta é a função central. A solução observa e aprende o padrão de comportamento "normal" do tráfego da sua rede (quem se comunica com quem, quais tipos de dados são trocados, volumes, horários, etc.). Ao invés de buscar por ameaças conhecidas (como vírus já identificados), ela procura por qualquer desvio significativo desse padrão normal. Por exemplo, se um servidor que normalmente só se comunica internamente começar a enviar grandes volumes de dados para um destino externo desconhecido, a solução sinaliza essa anomalia. Isso permite a detecção de ataques de "dia zero" (ameaças nunca vistas antes) e comportamentos internos maliciosos.
- **Detecção, Análise e Resposta de Incidentes de Segurança da Informação:**
  - **Detecção:** Assim que um comportamento anômalo ou uma atividade suspeita é identificada, a solução gera um alerta.
  - **Análise:** Em seguida, ela coleta informações contextuais sobre o incidente (quem, o quê, onde, quando) para ajudar a entender a natureza da ameaça, seu impacto potencial e sua origem. Esta análise pode ser feita automaticamente pela plataforma e/ou por analistas de segurança.
  - **Resposta:** Com base na análise, a solução pode tomar ações automatizadas (como bloquear um endereço IP malicioso ou isolar um dispositivo comprometido) ou fornecer recomendações e ferramentas para que a equipe de segurança da empresa possa intervir e conter o incidente, minimizando danos e restaurando a segurança.
- **Baseado em Serviço (SOC-as-a-Service (Security Operations Center-as-a-Service):** Esta é a característica chave que diferencia esta contratação de uma solução "on-premises" (instalada na sua infraestrutura). No modelo SOC como seviço:
  - **Nuvem:** A solução é hospedada e gerenciada por um provedor de serviços externo, na nuvem. Você não precisa comprar, instalar, manter ou atualizar servidores e softwares.
  - **Assinatura:** Você paga uma taxa de assinatura (mensal ou anual) pelo uso do serviço, geralmente baseada no volume de dados monitorados, número de usuários ou outros métricas.
  - **Gerenciamento do Provedor:** O provedor de SOC como seviço é responsável pela infraestrutura, manutenção, atualizações de software, patches de segurança e, em muitos casos, parte da análise e gerenciamento dos alertas. Isso tira uma grande carga da equipe de TI/Segurança da empresa contratante.
  - **Acesso Remoto:** A gestão e o acesso à plataforma de monitoramento são feitos via navegador web ou aplicativo, de qualquer lugar com conexão à internet.

5.8.2.2. Em resumo, essa solução faz com que a CONTRATANTE utilize um serviço de segurança cibernética avançado, focado em identificar atividades incomuns e potencialmente maliciosas na sua rede. A principal vantagem é que todo o hardware, software e grande parte da gestão dessa solução são de responsabilidade do provedor, permitindo que sua equipe de TI e segurança se concentre em outras prioridades e na resposta efetiva aos incidentes, em vez de na manutenção da infraestrutura de segurança.

Vantagens:

- Não requer investimento em hardware e software: Você não precisa comprar servidores, appliances ou licenças de software caras. O custo é uma despesa operacional (OPEX) recorrente (assinatura mensal/anual), o que facilita o orçamento e o fluxo de caixa.
- Menos custos com infraestrutura: Evita gastos com energia, refrigeração, espaço físico em data centers para hospedar a solução.
- Implantação rápida: Como a infraestrutura já está pronta na nuvem do provedor, a ativação do serviço é muito mais rápida do que a instalação de uma solução local.
- Configuração simplificada: Muitas vezes, a configuração inicial é mais simples, focando na integração de logs e telemetria da sua rede para a plataforma SOC como seviço.
- Gerenciamento do provedor: O provedor SOC como seviço é responsável por toda a infraestrutura, manutenção, atualizações de software, aplicação de patches de segurança e escalabilidade.
- Foco na segurança, não na infraestrutura: Sua equipe de segurança pode dedicar mais tempo à análise de alertas, investigação de incidentes e resposta às ameaças reais, em vez de se preocupar com a gestão da ferramenta em si.
- Adaptação ao crescimento: A solução na nuvem pode escalar rapidamente para acompanhar o crescimento do volume de dados da sua rede ou o aumento do número de usuários, sem que você precise adquirir ou provisionar mais recursos de hardware.
- Capacidade sob demanda: Você pode ajustar a capacidade de acordo com suas necessidades, o que é ideal para ambientes com flutuações de tráfego.
- Recursos avançados: Provedores SOC como seviço investem pesadamente em Machine Learning, Inteligência Artificial e inteligência de ameaças (threat intelligence) para aprimorar a detecção. Você se beneficia dessas inovações sem custo extra.
- Atualizações automáticas: A solução é atualizada e aprimorada constantemente pelo provedor, garantindo que você sempre tenha as defesas mais recentes contra novas ameaças.
- Equipe especializada do provedor: Muitos provedores de SOC como seviço oferecem equipes de especialistas (como um SOC as a Service) que podem auxiliar na análise de alertas e resposta a incidentes.
- Alta disponibilidade: Provedores de nuvem geralmente operam com redundância e robustos planos de recuperação de desastres, garantindo que o serviço de segurança esteja sempre disponível.

Desvantagens:

- Risco de interrupção: A solução exige uma conexão constante, estável e de alta largura de banda com a internet para que os dados da sua rede sejam enviados para a nuvem para análise. Se a conexão cair, a capacidade de monitoramento será comprometida.
- Dados fora de controle direto: Informações sensíveis sobre o tráfego da sua rede (metadados, logs) são enviadas e processadas na infraestrutura do provedor na nuvem.
- Conformidade regulatória: Pode haver desafios em relação à conformidade com leis de proteção de dados (como LGPD no Brasil, GDPR na Europa), dependendo de onde os dados são armazenados e processados pelo provedor. É crucial revisar os contratos e certificações.
- Custo acumulado: Embora os custos iniciais sejam baixos, a longo prazo (vários anos), o valor total das assinaturas pode ser superior ao de uma solução local adquirida e mantida pela própria empresa, especialmente para grandes volumes de dados.
- Limitação de customização: Você tem menos controle sobre a infraestrutura subjacente e as configurações de baixo nível da solução. A personalização é limitada às opções que o provedor oferece através de sua interface.
- Integrações específicas: Alterações ou integrações muito específicas com outros sistemas internos podem depender da disponibilidade de APIs ou da roadmap do provedor.
- A solução pode ter dificuldade em inspecionar o conteúdo de tráfego criptografado (HTTPS, VPNs) sem medidas adicionais (como proxies de descriptografia na sua rede antes de enviar os dados para a nuvem), o que pode deixar "pontos cegos" para ameaças que se escondem na criptografia.
- Migrar de um provedor SOC como seviço para outro pode ser complexo, pois os dados, configurações e modelos de detecção estão integrados à plataforma do provedor atual.
- O envio de dados da sua rede para a nuvem e o processamento podem introduzir uma latência mínima. Para detecção de anomalias, isso geralmente não é um problema crítico, mas é um fator inerente a qualquer serviço baseado em nuvem.

5.8.3. Análise Comparativa (Benchmarking)

- **Vectra:** https://www.vectra.ai/
- **Darktrace:** https://www.darktrace.com/
- **ExtraHop (RevealX):** https://www.extrahop.com/
- **Check Point Software:** https://www.checkpoint.com/pt/infinity/ndr/
- **Trend Micro: Foco:** https://www.trendmicro.com/pt_br/what-is/xdr/ndr.html
- **Stellar Cyber:** https://stellarcyber.ai/
- **Palo Alto Networks (Cortex XDR):** https://www.paloaltonetworks.com/

5.8.4. **Solução 3: Implantação de uma solução de software livre.**

5.8.4.1. Este modelo prevê a utilização de softwares de código aberto.

5.8.4.2. Análise da Solução: Não há disponibilidade de solução de software livre capaz de atender aos requisitos técnicos nesse contexto. Esta solução apresenta alta complexidade, pois necessita de capacitação permanente da equipe de informática, falta de suporte técnico, baixa cobertura para malwares e não prevenção de novos incidentes de segurança. Além dessas dificuldades, o volume de tráfego de rede vem crescendo cada ano exigindo hardwares dedicados para essa função. Assim, esta opção está aos poucos sendo substituída por ferramentas pagas com suporte, gerenciamento unificado e garantia de funcionamento.

Vantagens:

- Custo Inicial Reduzido/Grátis: A principal vantagem do software de código aberto é que ele geralmente não envolve custos de licenciamento inicial.
- Flexibilidade e Customização: O código aberto permite que as equipes modifiquem e adaptem o software às suas necessidades exatas, algo que muitas vezes é restrito em soluções proprietárias.
- Transparência: O código ser aberto permite uma auditoria de segurança e funcionalidade mais profunda, o que pode ser uma vantagem para organizações preocupadas com a segurança ou a forma como o software opera.
- Comunidade Ativa: Muitas soluções de código aberto têm comunidades vibrantes que oferecem suporte, documentação e desenvolvimento contínuo.

Desvantagens:

- Falta de Solução Adequada: Não há disponibilidade de solução de software livre capaz de atender aos requisitos técnicos.
- Alta Complexidade: A solução é complexa de implementar e gerenciar.
- Necessidade de Capacitação Permanente: A equipe de TI precisaria de treinamento contínuo para lidar com o software de código aberto, o que implica em custos e tempo.
- Falta de Suporte Técnico: Um ponto crucial. Soluções de código aberto frequentemente não oferecem o mesmo nível de suporte técnico formal e garantido que as soluções pagas possuem. O suporte depende da comunidade, que pode não ser ágil ou focada nas necessidades específicas da organização.
- Baixa Cobertura para Malwares: Para um contexto de segurança (implícito na menção de "malwares" e "segurança"), não é eficaz na proteção contra ameaças.
- Não Prevenção de Novos Incidentes de Segurança: Implica que a solução é reativa, e não proativa, na gestão de riscos de segurança.
- Demanda por Hardware Dedicado: O aumento do volume de tráfego de rede exige hardware específico, e o código aberto pode não otimizar o uso desse hardware tão bem quanto soluções proprietárias.
- Tendência de Substituição: O mercado está migrando de soluções de código aberto para ferramentas pagas que oferecem suporte, gerenciamento unificado e garantia de funcionamento, indicando que o código aberto está se tornando obsoleto para essa função específica.

5.8.5. **Análise Comparativa (Benchmarking)**

- **Bluefish**: https://bluefish.openoffice.nl/
- **MS2 Consulting (Brasil)**: https://ms2consulting.com.br/
- **H2L Soluções para Documentos (Brasil):** https://www.h2l.com.br/
- **FreeSoft:** https://freesoftbr.com/

5.8.6. **Análise comparativa das Soluções do cenário 1**

5.8.7. A Solução 1, baseada na contratação de um appliance dedicado de segurança (Network Detection and Response - NDR), apresenta um conjunto robusto de capacidades que a destaca frente às demais alternativas. Esta solução atua diretamente na infraestrutura da CONTRATANTE, oferecendo visibilidade em tempo real sobre todo o tráfego da rede, com análise comportamental baseada em inteligência artificial e machine learning. Sua arquitetura permite identificar e responder rapidamente a comportamentos anômalos, ameaças desconhecidas (ataques de dia zero), movimentos laterais e atividades suspeitas dentro da rede. A entrega via appliance garante alto desempenho e simplifica a implantação, pois o equipamento é pré-configurado e otimizado para funções de segurança, reduzindo o tempo de entrada em operação e minimizando riscos de configuração inadequada.

5.8.8. Além disso, a Solução 1 permite resposta automatizada a incidentes, integração com outras ferramentas de segurança (como EDRs e firewalls), e oferece suporte à conformidade com normativas de proteção de dados ao operar diretamente no ambiente da organização, o que proporciona maior controle sobre a análise e o armazenamento de dados sensíveis. Ainda que apresente um custo inicial mais elevado, trata-se de um investimento em segurança estratégica, com ganhos significativos em confiabilidade, tempo de resposta e cobertura técnica. O benchmarking evidenciou sua aderência a padrões internacionais e a presença de múltiplos fornecedores consolidados no mercado, como Darktrace, Vectra AI, ExtraHop, Fortinet e Cisco.

5.8.9. A Solução 2, por sua vez, adota o modelo SOC como seviço, oferecendo vantagens operacionais como baixo custo inicial, rápida implementação, atualizações automáticas e escalabilidade sob demanda. Contudo, a dependência de conectividade constante com a internet, a latência no envio e análise de dados em nuvem, e as restrições quanto ao controle direto sobre dados sensíveis representam desafios importantes. Questões regulatórias, especialmente frente à LGPD, e limitações quanto à inspeção de tráfego criptografado e customizações específicas, reduzem sua atratividade no contexto da CONTRATANTE.

Embora essa abordagem seja moderna e eficiente em ambientes mais dinâmicos ou de menor criticidade, sua adoção para redes de missão crítica e com elevado volume de tráfego pode implicar em riscos operacionais e de conformidade.

5.8.10. Por fim, a Solução 3, baseada em software livre, foi considerada tecnicamente inviável para atender à demanda. A inexistência de ferramentas gratuitas com maturidade tecnológica suficiente, somada à alta complexidade de implantação, à necessidade de equipe especializada, à falta de suporte contínuo, à cobertura limitada contra malwares e à ausência de mecanismos automatizados de resposta, inviabiliza sua adoção. Além disso, os crescentes volumes de tráfego exigiriam investimentos adicionais em infraestrutura física, comprometendo a suposta economia inicial e gerando riscos significativos de manutenção, desempenho e disponibilidade.

5.9. CENÁRIO 2 - Solução de Infraestrutura de rede Hardware e Software

5.9.1. Solução 1 - Componentes de Hardware para a captura e o monitoramento de tráfego sem a interceptação do conteúdo.

- **Hardware:** comumente, soluções para captura e o monitoramento de tráfego, sem a interceptação do conteúdo, são construídas através de arquiteturas de rede, composta por equipamentos de comutação que espelham tráfego. Soluções de cópia do tráfego de rede dependem de outros equipamentos idênticos e topologias específicas para poderem escalar. Nesse âmbito, as soluções não fornecem o nível de abordagem específico para analisar o conteúdo do tráfego existente, apenas copiam a informação bruta capturada.
- Interceptação passiva do tráfego - interfaces ópticas: para soluções e cópia de tráfego de rede, não é comum permitir a interceptação do tráfego ativo a nível de aplicação, de modo que se faz apenas possível analisar cabeçalhos de pacotes.
- Módulo de expansão para a captura do tráfego “inline”: a escalabilidade dessas soluções depende da construção de arquiteturas integradas, com o correto desvio de tráfego e sem um elemento central de rede para processar todo o tráfego e filtrá-lo corretamente. Nesse tipo de arquitetura, as ferramentas de segurança são otimizadas somente através de um elemento terceiro, um middleware, pois as informações abrangentes que serão recebidas serão orientadas, tão somente, a cabeçalhos de pacote.
- **Software:** para a camada de software, as soluções de rede são orientadas ao monitoramento e a captura do tráfego, tradicionalmente, até a camada 4. Nesse âmbito, apesar da possibilidade de construção de arquiteturas em que o tráfego possa ser analisado em sua completude, a solução irá carecer dos elementos necessários a otimização de todo o ferramental de segurança do PRODERJ, ela atuará somente como uma ferramenta de cópia do tráfego.
- Serviço técnico especializado para instalação, configuração, monitoramento da solução:
- Serviço técnico especializado para instalação, configuração, monitoramento da solução: Este é o serviço de profissionais especializados para auxiliar na implantação da solução. Dada a complexidade e a criticidade em copiar e desviar tráfego de rede, ter expertise para instalar o hardware, configurar o software, otimizar as políticas de integração com middlewares, em alguns casos, até mesmo ajudar no monitoramento inicial é fundamental para garantir o sucesso e a eficácia da solução.
- **Resumo:**
- Soluções tão somente orientadas a rede carecem do ferramental específico de redução de dados, filtro de aplicações e controle do fluxo específico de informações, como metadados, para otimizar o transporte de informações para ferramentas de processamento de segurança.
- O emprego de equipamentos de rede com o intuito de filtrar pacotes, de camada 2 a camada 7, não fornece o ferramental necessário a filtragem correta do tráfego presente.
- Soluções de rede se limitam ao roteamento e a comutação de pacotes, o uso de técnicas mais avançadas que envolvem a apuração de metadados e descriptografia do tráfego tem de ser complementadas por outros módulos auxiliares.
- Apesar de uma alternativa técnica, a sua viabilidade de execução, para o contexto específico dessa contratação, se encontra na contramão qualitativa com os resultados esperados pelo PRODERJ.

5.10. Análise Comparativa (benchmarking)

- Cisco Nexus Switches: https://www.cisco.com/site/us/en/products/networking/cloud-networking-switches/index.html
- Arista EOS Switches: https://www.arista.com/en/products/platforms
- Juniper: https://www.juniper.net/br/pt/products/switches.html
- Huawei Cloud Engine: https://e.huawei.com/za/products/switches/data-center-switches
- Mellanox: https://www.nvidia.com/en-in/networking/ethernet/switch-software/

Marca	Cisco	Arista	Juniper	Huawei	Mellanox
Captura passiva do tráfego	Sim	Sim	Sim	Sim	Sim
Captura ativa do tráfego	Não(Requer elemento adicional para processar os dados)				
Análise de Aplicações	Não(Requer elemento adicional para processar os dados)				

Desduplicação do Tráfego	Sim(Requer solução adicional de software para Packet Broker)	Sim(Requer solução adicional de software para Packet Broker)	Não	Não	Não
Análise de Metadados do Tráfego	Não(Requer solução adicional)				
Solução para Captura de Tráfego Virtualizada	Sim(versão virtual do sistema operacional)	Sim(versão virtual do sistema operacional)	Não	Não	Não

5.11. Por conseguinte, se torna explicito, que a solução 01 referenciada para o Lote 02 não atende as exigências técnicas e qualitativas do PRODERJ.

Solução 2: Componentes de Hardware e Interceptação de Tráfego e Licenciamentos integrados.

- Para a contratação da solução de interceptação do tráfego, a estrutura que definiu todos os itens fora elaborada conforme a extensa pesquisa de mercado entre os diversos fabricantes que comercializam esse tipo de solução.

A seguir, detalhamos o resultado de nossa pesquisa (benchmarking), que esclarece a estrutura da contratação:

ID	FABRICANTE	CISCO	ARISTA	GIGAMON	KEYSIGHT	NETSCOUT	APCON
	SOLUÇÃO	Cisco Nexus Data Broker	DANZ Monitoring Fabric	GigaVue	Ixia	nGenius	APCON
CARACTERÍSTICAS DA CONTRATAÇÃO DO PRODERJ							
1	POSSUI HARDWARE MODULAR	Sim (Nexus 3000/9000)	Sim (Arista M-100)	Sim (GigaVUE-HC, GigaVUE-TA Series)	Sim (Vision Edge 40 / Vision One / Vision X)	Sim (Chassis modular - Packet Flow Switch (PFS) 5000/7000 Series)	Sim (IntellaFlex XR Modular Chassis)
2	POSSUI LICENCIAMENTO DE DESDUPLICAÇÃO	Sim (Nexus Data Broker (NDB) Software)	Sim (DANZ Monitoring Fabric)	Sim (GigaSMART Deduplication)	Sim (Vision Series)	Sim (Packet Flow Operating System)	Sim (TitanXR Software)
3	POSSUI LICENCIAMENTO PARA DESCRIPTOGRAFIA DO TRÁFEGO	Sim (Cisco SSL Appliance)	Sim (Arista MSS)	Sim (GigaSMART SSL/TLS Decryption)	Sim (Vision ONE / Vision X com SSL decryption)	Sim (nGenius Decryption Appliance)	Não Suporta
4	POSSUI LICENCIAMENTO PARA FILTRO DE APLICAÇÕES	Sim (Nexus Data Broker + NX-OS ACLs (Access Control Lists))	Sim (Arista DMF + EOS)	Sim (Application Intelligence)	Sim (AppStack e Application Intelligence)	Sim (PFOS + nGeniusONE)	Sim (TitanXR)
5	POSSUI LICENCIAMENTO PARA FILTRO DE METADADOS DE APLICAÇÕES	Sim (Cisco Tetration)	Sim (Arista DMF Analytics Engine)	Sim (GigaSMART Metadata Generation)	Sim (AppStack + PacketStack)	Sim (nGeniusONE)	Sim (NetFlow Export - requer integração externa)
6	PERMITE A EXPANSÃO DA CAPACIDADE DE	Sim (Escalabilidade	Sim (O equipamento	Sim (Escalabilidade	Sim (Via módulos e	Sim (Permite	Apenas expansão de

	PROCESSMENTO	Horizontal)	possui formato de Chassi e permite a sua expansão)	Horizontal)	escalabilidade horizontal)	escalabilidade vertical e clusterização)	portas
7	POSSUI MÓDULO PARA A CAPTURA DO TRÁFEGO "EM-LINHA"	Sim (Cisco Bypass TAPs)	Sim (Fail-open interfaces ou via Integração com terceiros)	Sim (GigaSMART Bypass Protection)	Sim (Ixia iBypass)	Sim (Active Bypass TAPs)	Sim (APCON TAPs)
8	POSSUI GERENCIAMENTO CENTRALIZADO	Sim (Nexus Data Broker)	Sim (Arista DMF Controller)	Sim (GigaVUE-FM)	Sim (Fabric Controller)	Sim (nGenius Packet Flow Manager)	Sim (TitanXR GUI)
9	POSSUI APPLIANCE VIRTUAL PARA INTERCEPTAR TRÁFEGO	Não	Sim (Arista vDMF (Virtual DANZ Monitoring Fabric))	Sim (GigaVUE-VM)	Sim (Vision Virtual NPB)	Sim (vSTREAM)	Não Possui
10	POSSUI INTERCONECTORES PASSIVOS PARA CAPTURA DE TRÁFEGO (MÓDULO FÍSICO)	Sim (Network TAP Modules)	Sim (Arista Optical TAPs)	Sim (G-TAP)	Sim (Ixia Bypass TAPs e Optical TAPs)	Sim (nTap Passive TAPs)	Sim (Bypass TAPs)
11	POSSUI HARDWARE CONCENTRADOR DE TRÁFEGO (EQUIPAMENTO FOCADO EM INTERCEPTAÇÃO DE TRÁFEGO, COM MENOR PODER DE PROCESSAMENTO)	Sim (Nexus Switches + NDB Software)	Sim (Arista Packet Broker + DMF)	Sim (GigaVUE-TA Series)	Sim (Vision ONE / Vision Edge / Vision X)	Sim (PFS 5000/7000 Series)	Sim (IntellaFlex XR + TitanXR)
PONTUAÇÃO		10 / 11	11 / 11	11 / 11	11 / 11	11 / 11	8 / 11

Fontes

https://www.gigamon.com/products.html

https://www.keysight.com/us/en/products/network-visibility.html

https://www.arista.com/en/products/danz-monitoring-fabric

https://www.cisco.com/c/en/us/support/cloud-systems-management/nexus-data-broker/tsd-products-support-series-home.html

https://www.netscout.com/products/packet-flow-switches

https://www.apcon.com/products/intellaflex-xr/

1) Face ao exposto, destacamos que uma vez que existem, ao menos, 4 (quatro) soluções de mercado aderentes ao escopo pretendido, o PRODERJ optou por segmentar os itens que compõem a tabela do objeto.
2) Uma vez que a solução é modular, tanto a nível de hardware, quanto a nível de software, seja para sua expansão de recursos ou a expansão de funcionalidades técnicas, a sua segmentação permite ao PRODERJ não só o aporte financeiro conforme a melhor arquitetura prevista, como também flexibilidade nas tecnologias a serem adquiridas.
    a) Perante a necessidade de implantação da solução, principalmente no que tange a camada física e, concomitantemente, a capacidade de ativarmos as funcionalidades que melhor se adequam ao contexto de execução (desduplicação, filtro de aplicações, descriptografia de tráfego ou análise de metadados de aplicações), não se justifica a aquisição inicial de uma solução modular com tudo aquilo que ela fornece.
    b) Uma vez que exista a possibilidade de investimento naquilo que atenda o contexto específico do PRODERJ no tempo e, por conseguinte, sem a necessidade de aquisição completa inicial, a segmentação é preferível.

c) Torna-se factível "*itemizar*" os elementos técnicos, dentro de uma solução indivisível, para que então o PRODERJ possa consumir sob demanda todos os elementos que formam a solução no decorrer do contrato, sem prejuízo a equidade técnica no amparo da disponibilização de múltiplos concorrentes que podem atender a oferta prevista.

3) Referente ao ID 20, se esclarece que eles representam componentes comuns de mercado, denominados *transceivers*, ou transceptores. Esses dispositivos eletrônicos permitem a conversão do sinal elétrico em sinal óptico e, comumente, todo fabricante de equipamento (hardware), costuma possuir sua própria matriz de homologação para esses componentes.

5.12. **Análise comparativa das Soluções do cenário 2**

5.12.1. Ao analisar as duas abordagens do Cenário 2, para interceptação do tráfego, a Solução 1, Solução com componentes de Hardware para a captura e o monitoramento de tráfego sem a interceptação do conteúdo e a Solução 2, composta por componentes de soluções otimizadas para a interceptação o tráfego em conjunto a camada de rede, observamos diferenças chave em sua concepção e operação.

5.12.2. A Solução 1, baseada unicamente em equipamentos de rede que não detém do foco em interceptação específica do tráfego, ainda que dotada de mecanismos como espelhamento ou cópia passiva do tráfego, não se revela tecnicamente apta a atender ao escopo integral o PRODERJ, com a devida eficácia e amplitude funcional, uma solução dedicada a interceptação do tráfego. Embora tais dispositivos permitam a replicação do tráfego de rede com vistas ao monitoramento, suas limitações estruturais e operacionais inviabilizam sua adoção como substituto legítimo em contextos de maior criticidade, complexidade ou exigência técnica. De início, cumpre destacar a inexistência, nesse tipo de solução, da capacidade para a agregação inteligente de tráfego, pois não há possibilidade de consolidação lógica e subsequente distribuição otimizada, de forma seletiva, às ferramentas de segurança, diagnóstico ou observabilidade de modo nativo. Por conseguinte, esse tipo de solução carece de mecanismos avançados de filtragem por critérios e suas capacidades ficam restritas à camada 2 ou, em alguns casos, à camada 3, limitando-se a filtros por VLAN, endereço IP ou porta física. Ademais, a solução não oferece suporte a operações de otimização e saneamento de tráfego, tais como deduplicação de pacotes redundantes, supressão de cabeçalhos desnecessários, ou ainda, a análise contextual de tráfego de aplicações de modo nativo. Por fim, referenciamos a incapacidade de interagir com sessões SSL/TLS. A solução não dispõe de mecanismo para descriptografia em tempo real, com ou sem a colaboração de chaves privadas, permitindo a visibilidade plena de comunicações seguras — algo absolutamente imprescindível, pois a criptografia é norma e não exceção de tráfego.

5.12.3. Em contraste, a Solução 2 (Modular) segue uma abordagem modular e "best-of-breed", permitindo a escolha de componentes especializados. A utilização de solução de interceptação do tráfego, como instrumentos centrais para a captura, tratamento e distribuição de tráfego de rede representa uma evolução tecnológica substancial frente ao emprego isolado de soluções convencionais de rede dotadas de funcionalidades básicas de espelhamento (como SPAN, RSPAN ou ERSPAN). Cumpre destacar a capacidade dessa solução de operar filtros de tráfego com elevada granularidade, alcançando a aplicação (L7-Camada de aplicação do Modelo OSI). Essa prerrogativa permite a seleção criteriosa de pacotes com base em atributos como IP de origem e destino, porta, protocolo, tipo de aplicação, geolocalização e até padrões de payload. Outra vantagem da solução reside em sua capacidade de agregação de múltiplas fontes de tráfego simultaneamente, sejam estas provenientes de conectores passivos físicos, enlaces redundantes, VLANs distintas, ambientes virtualizados ou segmentos encapsulados da rede. A solução também oferece funcionalidade de otimização e saneamento de pacotes, como a deduplicação de tráfego redundante — oriundo de múltimos pontos de captura — e a supressão de cabeçalhos desnecessários, garantindo que apenas pacotes essenciais, limpos e tratáveis sejam encaminhados às ferramentas analíticas. Adicionalmente, é relevante assinalar que esse tipo de solução incorpora funcionalidades de descriptografia SSL/TLS, viabilizando a inspeção de tráfego criptografado em tempo real — recurso indispensável frente ao crescimento exponencial da adoção de criptografia no tráfego corporativo. À luz de todo o exposto, a solução se apresenta como instrumento indispensável à arquitetura de redes modernas, especialmente em ambientes que demandam visibilidade precisa, controle refinado e segurança operacional contínua.

5.12.4. Em resumo: A Solução 2 é a ideal e indispensável para redes modernas, pois, ao contrário da Solução 1 (básica e limitada), ela permite filtros detalhados por aplicação (Camada 7), agregação e otimização de tráfego, e, crucialmente, a descriptografia de comunicações seguras em tempo real, garantindo controle e visibilidade completos.

5.13. **CENÁRIO 3 - Solução de Gerenciamento e Orquestração**

5.13.1. **Solução 1 - Elastic Cloud Enterprise - ECE e serviços especializados**

5.13.1.1. Trata-se de uma solução de Elastic Cloud Enterprise (ECE) é uma plataforma de gerenciamento e orquestração que permite a você implantar, escalar e gerenciar múltiplos clusters do Elastic Stack (que inclui Elasticsearch, Kibana, Logstash, Beats, e outros componentes como APM, Fleet, etc.) em qualquer infraestrutura: seja em servidores bare metal, máquinas virtuais (VMs), nuvens privadas ou zonas privadas de nuvens públicas (como AWS, Google Cloud, Azure). Em outras palavras, o ECE serve para simplificar e automatizar a operação do Elastic Stack em larga escala, em ambientes on-premise ou híbridos.

5.13.1.2. Aqui estão os principais propósitos e funcionalidades do ECE:

1) **Gerenciamento Centralizado de Múltiplos Clusters:**

- Permite a criação, gerenciamento e monitoramento de dezenas ou centenas de clusters Elasticsearch e suas respectivas instâncias Kibana a partir de uma única interface centralizada.
- Isso é ideal para grandes organizações que têm muitos times ou departamentos usando o Elastic Stack para diferentes casos de uso (observabilidade, segurança, busca, etc.).

1) **Automação do Ciclo de Vida do Cluster:**

- **Provisionamento:** Automatiza a criação de novos clusters e instâncias do Elastic Stack de forma rápida e consistente.
- **Escalonamento:** Permite adicionar ou remover nós (memória, CPU, disco) de um cluster de forma elástica, sem tempo de inatividade, para atender às demandas de dados e uso.
- **Upgrades:** Simplifica o processo de atualização de versões do Elastic Stack, garantindo que os clusters permaneçam atualizados com os recursos mais recentes e correções de segurança.
- **Backups e Restauração:** Gerencia a criação e restauração de snapshots (cópias de segurança) dos seus dados, protegendo contra perda de dados.

1) **Flexibilidade de Infraestrutura:**

   - O ECE é "agnóstico" da infraestrutura subjacente. Você pode implantá-lo em hardware físico, VMs, ou em nuvens privadas/públicas. Isso permite que as empresas utilizem sua infraestrutura existente e mantenham o controle sobre seus dados.

2) **Habilitar Múltiplos Casos de Uso:**

   - Com o ECE, as organizações podem gerenciar facilmente vários casos de uso do Elastic Stack, como:

     - **Observabilidade:** Coleta e análise de logs, métricas e traces de aplicações e infraestrutura (APM, Logs, Metrics).
     - **Segurança:** Detecção de ameaças, análise de eventos de segurança (SIEM), proteção de endpoints.
     - **Busca Empresarial:** Construção de motores de busca internos, busca em sites, aplicações de e-commerce.
     - **Análise de Dados:** Exploração de dados, machine learning, relatórios e dashboards.

3) **Multitenancy e Isolamento:**

   - O ECE facilita o multitenancy, permitindo que diferentes equipes ou projetos tenham seus próprios clusters isolados, com controle de acesso e recursos independentes. Isso ajuda a resolver desafios como retenção de dados e controle de versões para diferentes stakeholders.

4) **Recursos Avançados e Segurança:**

   - Permite o uso de recursos avançados do Elastic Stack (disponíveis nas assinaturas pagas do Elastic), como Machine Learning, Security (X-Pack Security), alerta, monitoramento, etc.
   - Oferece funcionalidades de segurança para a própria plataforma ECE (como controle de acesso baseado em função - RBAC, e autenticação externa) e para os clusters gerenciados.

5.13.1.3. Em resumo, o ECE é a solução da Elastic para empresas que precisam de uma forma robusta, automatizada e escalável de operar o Elastic Stack em sua própria infraestrutura, oferecendo uma experiência similar a um "Elastic Cloud privado". Ele remove grande parte da complexidade operacional associada ao gerenciamento manual de clusters Elasticsearch em grande escala.

- **O Serviço Técnico Especializado: Elastic Cloud Enterprise (ECE)**

O **serviço técnico especializado** para o **Elastic Cloud Enterprise (ECE)** é o suporte profissional que garante que sua organização tire o máximo proveito dessa plataforma.

Ele serve para:

- **Instalação e Configuração:** Ajuda a implantar e configurar o ECE corretamente em sua infraestrutura, garantindo performance e segurança.
- **Otimização:** Otimiza seus clusters Elastic (Elasticsearch, Kibana, etc.) para diferentes usos, como segurança ou observabilidade, garantindo que funcionem de forma eficiente.
- **Suporte e Monitoramento:** Oferece monitoramento proativo e ajuda a resolver problemas, além de auxiliar em upgrades e backups.
- **Capacitação:** Treina sua equipe para que ela possa gerenciar e operar o ECE de forma autônoma.

5.13.1.4. Em resumo, é a **expertise humana** que complementa a tecnologia do ECE, garantindo uma operação suave e eficiente do seu Elastic Stack em larga escala.

Vantagens:

- Gerenciamento Centralizado: Proporciona uma interface unificada para criar, gerenciar, monitorar e escalar múltiplos clusters Elasticsearch e Kibana a partir de um único painel.
- Automação do Ciclo de Vida: Automatiza tarefas complexas e repetitivas como provisionamento, escalonamento (adição/remoção de nós), upgrades de versão, backups e restauração de desastres, reduzindo significativamente o esforço operacional.
- Operações "One-Click": Muitas operações complexas são simplificadas para cliques na interface do usuário ou chamadas de API.
- Reaproveitamento de Infraestrutura: Permite utilizar seus próprios servidores (bare metal) ou VMs, aproveitando investimentos existentes em hardware.
- Maximização da Utilização de Hardware: O ECE é projetado para maximizar a utilização dos recursos dos seus hosts, consolidando múltiplos clusters em uma mesma infraestrutura de forma eficiente.
- Controle de Custos: Ao rodar na sua própria infraestrutura, você tem controle direto sobre os custos de hardware e licenças, evitando os custos variáveis e muitas vezes mais altos de serviços gerenciados em nuvem para cargas de trabalho pesadas e constantes.
- Escolha da Infraestrutura: Pode ser implantado em data centers próprios, nuvens privadas ou em regiões e contas específicas de nuvens públicas (AWS, Azure, GCP) onde a Elastic Cloud gerenciada pode não estar disponível ou não atender a requisitos específicos.

- Controle de Dados: Permite manter os dados dentro da sua rede interna, atendendo a requisitos de compliance, segurança e soberania de dados para informações regulamentadas ou sensíveis
- Customização Avançada: Oferece opções para criar templates de deployment personalizados, configurar alocadores, e integrar-se com a sua infraestrutura de rede e segurança existente.
- Suporta todos os recursos do Elastic Stack, incluindo Machine Learning, Security (X-Pack Security), observabilidade (Logs, Metrics, APM), busca empresarial, etc., com a mesma facilidade de deployment.
- Facilita a implementação de arquiteturas como "hot-warm" para gerenciamento de ciclo de vida de dados.
- Permite que diferentes equipes ou projetos tenham seus próprios clusters isolados e configurados com suas próprias necessidades de recursos e segurança.
- Proporciona isolamento de recursos entre os diferentes deployments, mitigando o "efeito vizinho barulhento" (noisy neighbor effect).

Desvantagens:

- Custo de Implantação: Embora reduza a complexidade operacional a longo prazo, a instalação inicial do ECE pode ser complexa e requer conhecimento técnico especializado, incluindo Docker, Kubernetes (indiretamente na arquitetura do ECE), redes e sistemas operacionais.
- Infraestrutura Subjacente: Você é responsável por provisionar, manter e gerenciar a infraestrutura de hardware/VMs onde o ECE será executado (servidores, rede, armazenamento, etc.).
- Atualizações do ECE: Embora o ECE simplifique os upgrades dos clusters do Elastic Stack, o upgrade da própria plataforma ECE ainda requer planejamento e execução cuidadosos.
- O ECE é um produto licenciado da Elastic, e o custo da licença pode ser significativo, especialmente para grandes implantações, pois geralmente está ligado à quantidade de memória provisionada.
- Requer uma assinatura paga da Elastic para acessar as funcionalidades completas e o suporte.
- Ao contrário do Elastic Cloud (o serviço gerenciado pela Elastic), o ECE não é um serviço SaaS. Você ainda é responsável pela operação e manutenção da plataforma ECE e da infraestrutura subjacente.
- Isso significa que a Elastic não gerencia diretamente o seu ECE; ela fornece o software e o suporte para você gerenciá-lo.
- Para operar o ECE de forma eficaz, sua equipe precisará ter expertise em administração de sistemas, redes, Docker e, claro, no Elastic Stack. Isso pode ser um desafio para equipes menores ou menos experientes.
- Como qualquer software complexo, o ECE pode ter limitações ou problemas conhecidos que exigem atenção e, às vezes, soluções de contorno. É importante consultar a documentação e os fóruns de suporte.

Análise Comparativa (Benchmarking)

Elastic: https://www.elastic.co/

5.13.2. **Solução 2 - Software splunk enterprise e serviços profissionais especializados**

5.13.2.1. O **Splunk Enterprise** é uma plataforma de software que **coleta, indexa, busca, analisa e visualiza grandes volumes de dados gerados por máquinas** em tempo real. Ele funciona como um "Google para seus dados de máquina", transformando informações não estruturadas de logs, aplicações e dispositivos em inteligência acionável.

5.13.2.2. Ele é utilizado principalmente para:

- **Observabilidade e Gerenciamento de Operações de TI (ITOM):** Monitora a infraestrutura e aplicações, ajuda na resolução de problemas e otimiza o desempenho.
- **Segurança da Informação (SIEM):** Detecta ameaças cibernéticas, auxilia na resposta a incidentes e garante a conformidade com regulamentações.
- **Inteligência de Negócios e Análise de Dados:** Oferece insights sobre o desempenho de processos de negócios e permite análise avançada com machine learning.

Os **Serviços Profissionais Especializados Splunk** são fornecidos por consultores e empresas experientes que ajudam organizações a maximizar seu investimento na plataforma. Eles atuam em diversas frentes:

- **Planejamento e Design:** Criam arquiteturas Splunk escaláveis e eficientes.
- **Implementação e Configuração:** Realizam a instalação, configuração e otimização do ambiente.
- **Desenvolvimento de Casos de Uso:** Criam dashboards, relatórios e alertas personalizados para atender a necessidades específicas.
- **Otimização e Treinamento:** Melhoram a performance do Splunk e capacitam as equipes internas.
- **Suporte Contínuo:** Garantem a operação e a saúde do ambiente Splunk.

5.13.2.3. Em resumo, o Splunk Enterprise é a ferramenta que transforma dados brutos em insights valiosos, e os Serviços Profissionais garantem que essa ferramenta seja implementada e utilizada de forma eficaz para resolver desafios complexos de TI e negócios.

Vantagens:

- Versatilidade de Dados: Consegue ingerir e processar praticamente qualquer tipo de dado de máquina (logs, métricas, eventos, dados estruturados/não estruturados) de qualquer fonte.
- Indexação Poderosa: Transforma dados brutos em informações pesquisáveis e correlacionáveis em tempo real, mesmo sem um esquema pré-definido.
- SPL (Splunk Processing Language): Uma linguagem de busca e análise muito flexível e poderosa, permitindo extrair insights complexos e criar visualizações ricas.
- Observabilidade: Essencial para monitoramento de infraestrutura, aplicações e resolução de problemas (troubleshooting) em TI.
- Segurança (SIEM): Forte capacidade de detecção de ameaças, investigação de incidentes e conformidade regulatória.
- Inteligência de Negócios: Permite a análise de dados operacionais para otimização de processos e tomada de decisão.
- Projetado para lidar com volumes massivos de dados (terabytes a petabytes por dia) em ambientes distribuídos.
- Alta disponibilidade e tolerância a falhas através de clustering de indexers e search heads.
- Splunkbase: Grande marketplace de aplicativos (Apps) e add-ons desenvolvidos pela Splunk e pela comunidade, que estendem a funcionalidade para casos de uso específicos ou para integração com outras tecnologias.
- APIs: Facilita a integração com outras ferramentas e sistemas de TI.
- Mesmo com a complexidade subjacente, a interface do usuário permite criar dashboards e relatórios interativos para diferentes públicos.

Desvantagens:

- Licenciamento Baseado em Ingestão: O modelo de licenciamento é geralmente baseado na quantidade de dados ingeridos por dia, o que pode se tornar extremamente caro para grandes volumes, sendo um dos maiores desafios para muitas organizações.
- Custo de Infraestrutura: Requer hardware robusto e significativo para indexar e armazenar grandes volumes de dados, aumentando os custos de infraestrutura.
- Requer Expertise: A instalação, configuração e otimização de um ambiente Splunk Enterprise em larga escala exigem conhecimentos especializados em arquitetura distribuída, redes, sistemas operacionais e, claro, no próprio Splunk (SPL, apps, etc.).
- Gerenciamento Operacional: A manutenção contínua, upgrades, gerenciamento de capacidade e troubleshooting do próprio ambiente Splunk podem ser complexos e demorados.
- Embora poderosa, a Splunk Processing Language (SPL) tem uma curva de aprendizado inicial, especialmente para usuários novos em ferramentas de análise de logs e dados.
- A indexação em tempo real e a capacidade de pesquisa rápida consomem recursos significativos (CPU, RAM, I/O de disco), especialmente para consultas complexas ou grandes volumes de dados.
- Para algumas organizações, as desvantagens de custo e complexidade podem levar à exploração de alternativas de código aberto (como o Elastic Stack/ELK) ou soluções mais especializadas e talvez mais acessíveis para casos de uso específicos.

Análise Comparativa (Benchmarking)

Splunk: https://www.splunk.com/

5.14. **Análise comparativa das Soluções do cenário 3**

5.14.1. No contexto do presente estudo técnico, foram analisadas duas soluções amplamente consolidadas no mercado para tratamento e análise de dados operacionais, observabilidade, segurança da informação e busca empresarial: a Solução 1, baseada no Elastic Cloud Enterprise (ECE), e a Solução 2, fundamentada no uso do Splunk Enterprise com serviços profissionais especializados.

5.14.2. A Solução 1 – Elastic Cloud Enterprise (ECE) apresenta-se como uma plataforma robusta de orquestração e gerenciamento centralizado de múltiplos clusters do Elastic Stack (incluindo Elasticsearch, Kibana, Logstash, APM, entre outros). Ela permite que uma organização implante, escale e administre seu ecossistema Elastic em qualquer tipo de infraestrutura — seja local, em nuvem privada ou híbrida — com alto grau de automação e controle. Suas funcionalidades de provisionamento automático, escalonamento horizontal elástico, atualização simplificada, isolamento entre ambientes (multitenancy), e compatibilidade com todos os recursos premium da Elastic (como machine learning, SIEM e observabilidade distribuída) a tornam uma solução extremamente completa para grandes instituições públicas ou privadas que desejam manter seus dados sob domínio direto, sem abrir mão da elasticidade e da padronização operacional típicas de soluções SaaS.

5.14.3. Por sua vez, a Solução 2 – Splunk Enterprise é uma ferramenta poderosa para ingestão, indexação, análise e visualização de dados de máquina em tempo real. É altamente versátil, com forte atuação em observabilidade e segurança da informação (SIEM), e apresenta recursos avançados como a SPL (linguagem própria de consulta e análise), clustering tolerante a falhas e um amplo marketplace de integrações. No entanto, a solução é altamente dependente de licenciamento baseado em volume diário de ingestão de dados, o que pode tornar sua adoção financeiramente inviável para cenários com grande volume de eventos contínuos (como ambientes públicos com múltiplas fontes de log distribuídas). Além disso, sua instalação e operação exigem conhecimento técnico especializado, além de investimento contínuo em serviços profissionais para manutenção e personalização de uso.

5.14.4. Do ponto de vista técnico, a Solução 1 se mostra mais vantajosa por oferecer:

a) Maior controle da infraestrutura e dos dados, permitindo atender com maior facilidade aos requisitos de soberania, sigilo e conformidade regulatória;

b) Flexibilidade de implantação, podendo ser usada em servidores existentes ou ambientes híbridos, o que possibilita o reaproveitamento de investimentos prévios em hardware e virtualização;

c) Isolamento de ambientes, com suporte a múltiplos clusters independentes, o que permite atender diferentes áreas ou órgãos com níveis de segurança e recursos distintos;

d) Custo previsível, baseado em recursos provisionados e não em volume de ingestão, o que favorece cargas de trabalho contínuas e pesadas típicas de ambientes públicos;

e) Acesso nativo a recursos avançados do Elastic Stack, como detecção automatizada de anomalias, análise de logs e métricas, APM distribuído, e segurança da informação com recursos de SIEM;

f) Interface unificada e APIs para automação, reduzindo drasticamente a complexidade de gerenciamento operacional em larga escala.

5.14.5. Embora o Splunk Enterprise possua reconhecida excelência em segurança e análise de logs, seu modelo de licenciamento baseado em ingestão, somado ao custo elevado dos serviços especializados, representa um obstáculo relevante para ambientes que exigem alta escalabilidade e ingestão contínua de grandes volumes de dados. Além disso, sua dependência de profissionais certificados para ajustes e expansão pode introduzir gargalos operacionais e financeiros.

6. ANÁLISE DE PROJETOS SIMILARES

6.1. Foram analisadas contratações similares formalizadas por outros órgãos e entidades, por meio de consultas ao sistema Painel de Preços do Portal de Compras do Governo Federal, com objetivo de identificar a existência de novas metodologias, tecnologias ou inovações que melhor atendessem às necessidades da Administração, e as que foram identificadas foram incorporadas na contratação em análise.

6.2. Na contratação em análise não foram identificadas situações específicas ou casos de complexidade técnica do objeto, que pudessem acarretar a realização consulta pública para coleta de contribuições a fim de definir a solução mais adequada visando preservar a relação custo-benefício, em face dos serviços serem considerados comuns.

6.3. CENÁRIO 1 - Solução de Segurança

6.3.1. Solução 1 - Contratações Similares - Solução de Network Detection and Response

ÓRGÃO PÚBLICO	CONTRATAÇÕES SIMILARES							
	DESCRIÇÃO SUCINTA		**QTD SOLICITADA**	**PREÇO UNITÁRIO**	**Atualização pelo ICTI * (7,10% - jan/25**	**PREÇO GLOBAL PROJETADO**	**PREÇO GLOBAL PROJETADO**	**PREÇO MÉDIO GLOBAL**
MINISTÉRIO DA CULTURA Pregão 90012/2024 EDITAL 110773277	Contratação de solução de tecnologia da informação e comunicação para realizar detecção, análise, resposta e monitoramento de incidentes de segurança da informação, conforme condições, quantidades - 36 meses	Solução de monitoramento de comportamento anômalo da rede, detecção, análise, resposta e restauração de incidentes de segurança da informação.	2	R$ 3.905.171,83	R$ 4.182.439,03	R$ 8.364.878,06	R$ 8.449.660,18	**R$ 9.096.101,97**
		Serviço de Implantação da solução	1	R$ 55.728,37	R$ 59.685,08	R$ 59.685,08		
		Treinamento da solução	6	R$ 3.905,55	R$ 4.182,84	R$ 25.097,04		
CÂMARA DOS DEPUTADOS 33/2022 110772712	Prestação de serviços de monitoramento e apoio à resposta a incidentes de segurança cibernética, de varredura de vulnerabilidades e de inteligência contra ameaças cibernéticas,	Serviço de monitoramento e apoio à resposta a incidentes de segurança cibernética	2	R$ 1.129.596,99	R$ 1.209.798,38 12 meses R$ 3.629.395,14 36 meses	R$ 7.258.790,28	R$ 8.026.900,92	

	incluindo capacitação operacional.- 12 meses	Serviço de inteligência contra ameaças cibernéticas	1	R$ 526.923,92	R$ 564.335,52	R$ 564.335,52		
		capacitação operacional na operação de software	6	R$ 31.711,04	R$ 33.962,52	R$ 203.775,12		
SEDUC/RO ATA 161/2023 110772678	Fornecimento de Solução Unificada de Segurança para proteção de e-mail, proteção de endpoint e proteção contra-ataquesavançados, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, paraatendimento das necessidades da Secretaria de Estado da Educação	Solução de segurança contra ameaças avançadas com detecção e resposta - item 7 da ATA	2	R$ 1.550.000,00	R$ 1.660.050,00 12 meses R$ 4.980.150,00 36 meses	R$ 9.960.300,00	R$ 10.811.745,00	
		Serviço Especializado de Instalação e configuração - item 9 da ATA	1	R$ 660.000,00	R$ 706.860,00	R$ 706.860,00		
		Serviço Especializado de Treinamento Hands-on - item 10 da ATA	6	R$ 22.500,00	R$ 24.097,50	R$144.585,00		

*Índice de custo da tecnologia da informação - IPEA (Índice e série histórica disponível neste link) **foi aplicado o índice nos pregões com mais de 01 (um) ano.**

Valor estimado Cenário 1 - Solução 1
Solução de Network Detection and Response
R$ 9.096.101,97

6.3.2. **Solução 2 - Contatações Similares - Contratação de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, baseado em serviço SOC-as-a-Service (Security Operations Center-as-a-Service).**

ÓRGÃO PÚBLICO	**CONTRATAÇÕES SIMILARES**				
	DESCRIÇÃO SUCINTA	**QTD SOLICITADA**	**PREÇO UNITÁRIO**	**Atualização pelo ICTI * (7,10% - jan/25**	**PREÇO MÉDIO GLOBAL**
MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA EDITAL DE LICITAÇÃO	Contratação de serviços de tecnologia da informação e comunicação, através da seleção de empresa especializada, para o fornecimento de Serviço de Centro de Operações de Segurança (Security Operations Center - SOC) com funcionamento e suporte 24h por dia e 7 dias por semana, Serviço de tratamento e resposta aos incidentes cibernéticos -	1	R$ 2.126.039,39 12 meses R$ 6.378.118,17 36 meses	R$ 6.830.964,56	**R$ 11.566.771,27**

PREGÃO ELETRÔNICO Nº 21/2021 110772825	CSIRT - Blue Team e Serviço de teste de invasão - Red Team pelo período de 24(vinte e quatro) meses.				
TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA EDITAL – PREGÃO ELETRÔNICO nº 048/2024 110774514	Contratação de Serviços Gerenciados de Segurança da Informação com Central de Operações de Segurança (Security Operations Center – SOC) no modelo Software as a Service (SaaS), incluindo Gestão de Vulnerabilidades, Gestão de Incidentes, Monitoramento e Visibilidade de ataques Cibernéticos, Testes de Invasão, Simulação de ataques relacionados à Segurança Digital, para o Tribunal de Justiça do Estado da Bahia - TJBA	1	R$ 5.073.942,73 12 meses R$ 15.221.828,19 36 meses	R$ 16.302.577,99	

OBS: Ministério da Justiça e Segurança Pública possui o valor de R$ 4.252.078,79 para 24 meses, foi dividido por 2 para chegar no valor de 12 meses (R$ 2.126.039,39) e depois multiplicado por 3 para chegar no valor de 36 meses (R$ 6.378.118,17)

OBS: Tribunal de Justiça Bahia possui o valor de R$ 10.147.885,46 para 24 meses, foi dividido por 2 para chegar no valor de 12 meses (R$ 5.073.942,73) e depois multiplicado por 3 para chegar no valor de 36 meses (R$ 15.221.828,19)

6.3.3. **Solução 2 - Treinamento para o SOC**

ÓRGÃO PÚBLICO	**CONTRATAÇÕES SIMILARES**				
	DESCRIÇÃO SUCINTA	**QTD SOLICITADA**	**PREÇO UNITÁRIO**	**PREÇO GLOBAL PROJETADO**	**PREÇO MÉDIO GLOBAL**
SEFA - SECRETARIA DE FAZENDA DO PARÁ PREGÃO ELETRÔNICO 90001 /2025 110776566	Treinamento da ferramenta de Monitoração de Eventos de Segurança	6	R$ 22.473,85	R$ 134.843,10	**R$ 97.421,55**
SECRETARIA MUNICIPAL DE FINANÇAS BENTO GONÇAVES - RS PREGÃO ELETRÔNICO nº 012/2025 110775965	Treinamento	6	R$ 10.000,00	R$ 60.000,00	

Valor estimado Cenário 1 - Solução 2
Contratação de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, baseado em serviço SOC-as-a-Service (Security Operations Center-as-a-Service). + Treinamento para o SOC
R$ 11.566.771,27 + R$ 97.421,55 = **R$ 11.654.192,82**

6.3.4. **Solução 3 - Contratações Similares - Implantação de uma solução de software livre.**

6.3.4.1. A Solução 3, baseada em software livre, foi considerada tecnicamente inviável para atender à demanda. A inexistência de ferramentas gratuitas com maturidade tecnológica suficiente, somada à alta complexidade de implantação, à necessidade de equipe especializada, à falta de suporte contínuo, à cobertura limitada contra malwares e à ausência de mecanismos automatizados de resposta, inviabiliza sua adoção. Além disso, os crescentes volumes de tráfego exigiriam investimentos adicionais em infraestrutura física, comprometendo a suposta economia inicial e gerando riscos significativos de manutenção, desempenho e disponibilidade.

6.4. **CENÁRIO 2 - Solução de Infraestrutura de rede Hardware e Software**

6.4.1. **Solução 1 - Componentes de Hardware para a captura e o monitoramento de tráfego sem a interceptação do conteúdo**

6.4.2. Conforme elencado dentro do nosso Levantamento de Mercado e na seção de benchmarking da solução, qualitativamente, esse tipo de solução está aquém das qualidades técnicas esperadas pelo PRODERJ.

6.4.3. Não obstante, apesar de identificados múltiplos processos públicos, nenhum dele possui alcunha complementar para a interceptação de tráfego, fosse com componentes nativos da oferta, fosse com middlewares complementares.

6.4.3.1. **Contratações Similares - Solução 1**

ÓRGÃO PÚBLICO	DESCRIÇÃO SUCINTA	PREÇO UNITÁRIO	Atualização pelo ICTI * (7,10% - jan/25	QTD SOLICITADA	PREÇO GLOBAL
Superior Tribunal de Justiça Pregão Eletrônico 139/2023 (itens 41,42 e 43) 110777614	Switch Tipo IV - Datacenter	R$ 157.587,28	R$ 168.775,98	4	R$ 675.103,92
	Serviço de suporte técnico para Switch Tipo IV - Datacenter	R$ 31.312,65	R$ 33.535,85	4	R$134.143,40
	Instalação de Switch Tipo IV	R$ 15.869,72	R$ 16.996,47	4	R$ 67.985,88
Empresa de Tecnologia da Informação e Comunicação do Estado do Pará – PRODEPA Pregão Eletrônico 02/2023 (itens 1,2,3, 19 e 20) 110777608	Comunicação LAN/Ethernet de Alto Desempenho – Spine (Switch LAN – Tipo 1)	R$ 200.663,83	R$ 214.910,96	4	R$ 859.643,84
	Comunicação LAN/Ethernet de Alto Desempenho – Leaf (Switch LAN – Tipo 2)	R$ 170.216,12	R$182.301,46	4	R$ 729.205,84
	Comunicação LAN/Ethernet de Alto Desempenho – Leaf (Switch LAN – Tipo 3)	R$ 256.420,25	R$ 274.626,08	4	R$ 1.098.504,32

	Serviço de Instalação e Configuração para Comunicação LAN/Ethernet de Alto de Desempenho – Switch Core Datacenter – Modelo Spine	R$ 19.000,00	R$ 20.349,00	4	R$ 81.396,00
	Serviço de Instalação e Configuração para Comunicação LAN/Ethernet de Alto de Desempenho – Switch Core Datacenter – Modelo Leaf	R$ 18.999,99	R$ 20.348,99	4	R$ 81.395,96
Departamento de policia federal 200342 - diretoria de tecn.da informação e inovação relação de itens - pregão eletrônico nº 90006/2024-000 srp 110777455	Serviço de suporte técnico especializado	R$ 398,25	R$ 426,52	3.238	R$ 1.381.071,76
Tribunal de Contas do Distrito Federal Pregão Eletrônico Nº 17/2023 110777934	Prestação de serviços técnicos especializados, sob demanda (por meio de Ordem de Serviço – O.S.), de acordo com catálogo de serviços	R$ 415,53	R$ 445,03	3.238	R$ 1.441.007,14

ITEM	PREÇO MÉDIO ESTIMADO UNITÁRIO	QTDE	PREÇO MÉDIO GLOBAL ESTIMADO
Equipamento para a interceptação do tráfego (*) + Serviço de suporte técnico para Switch	R$ 210.153,62 + R$ 22.807,58	4	R$ 31.842,32
Serviço Técnico Especializado	R$ 435,77	3.238	R$ 1.411.023,26

(*)Equipamento para a interceptação do tráfego - faz referência aos Switchs Tipo 1,2,e e 4 da tabela Contratações Similares - Solução 1 foram somados os valores e dividido por 4 para encontrar o preço médio R$ 210.153,62 + serviço tecnico R$ 22.807,58.

OBS: Ressaltamos que a pesquisa aponta processos que compreendem uma solução não aderente ao escopo de atendimento do contexto do PRODERJ. Apesar da facilidade de identificação de soluções de rede, o seu contexto complementar para interceptação do tráfego, seja de modo integrado, seja através de middlewares, não foi identificado.

Valor estimado Cenário 2 - Solução 1
Componentes de Hardware para a captura e o monitoramento de tráfego sem a interceptação do conteúdo
R$ 2.342.865,58

6.4.4. **Solução 2 - Componentes de Hardware e Interceptação de Tráfego e Licenciamentos integrados.**

6.4.4.1. Após extensa pesquisa dentro dos contratos federais (comprasnet), e nos portais estaduais, não foram identificadas contratações com o mesmo escopo, nem similar nem idêntica, ao desta contratação determinada neste Estudo Técnico. Alguns projetos foram identificados, entretanto, eles não cumprem a exigência técnica desta contratação.

6.4.4.2. Em consonância a não identificação de referências de preço através de processos governamentais homologados, fora buscado em mídia especializada (domínios públicos na internet), possíveis aferições de preço que subsidiassem este Estudo Técnico preliminar.

6.4.4.3. Como fontes de pesquisa, foram buscadas referências de preços dos fabricantes, como:

- Cisco;
- Arista;
- Gigamon;
- KeySight;
- NetScout.

6.4.4.4. Tendo em vista que a pesquisa se pautou no uso de URLs públicas, com possíveis preços de lista de soluções aderentes ao escopo, as tabelas a seguir detêm de todas as fontes consultadas na análise.

6.4.4.5. Itens não identificados, em perspectiva a aqueles correlatos ao processo, foram registrados nas tabelas como “Não encontrado”, por não terem uma referência pública de fácil aferição.

6.4.4.6. Utilizaremos as informações expostas a seguir como uma referência, tão somente, de aquisição da solução pretendida abaixo.

6.4.5. **Contratações Similares - Solução 2**

PESQUISA FABRICANTE NETSCOUT											
CATÁLOGO	**ITEM**	**DESCRIÇÃO**	**SKU**	**DESCRIÇÃO**	**QTD**	**CUSTO UNITÁRIO**	**IMPOSTO TOTAL DE IMPORTAÇÃO DE HARDWARE (PJ)**	**IMPOSTO TOTAL DE IMPORTAÇÃO DE SOFTWARE (PJ)**	**CUSTO COM IMPORTAÇÃO**	**CUSTO UNITÁRIO TOTAL**	**CUSTO UNITÁRIO EM MOEDA NACIONAL**
https://www.shi.com	4	Equipamento para a interceptação do tráfego, com 36 (trinta e seis) meses de garantia oficial da fabricante	50FCNANQH0J0	NetScout nGenius 5000 Series Packet Flow Switch 5010	2	USD 41.396,00	70%	0%	USD 28.977,20	USD 70.373,20	R$ 382.830,21
https://www.insight.com	5	Licenciamento de desduplicação do tráfego, com 36 (trinta	51401L-VAAS	NETSCOUT Systems nGenius PFS Fabric	2	USD 18.664,95	0%	30%	USD 5.599,49	USD 24.264,44	R$ 131.998,53

		e seis) meses de subscrição e garantia oficial da fabricante		Manager - license							
https://www.insight.com	6	Licenciamento avançado de descriptação do tráfego, com 36 (trinta e seis) meses de subscrição e garantia oficial da fabricante	C-09807-M0S-2-1M	NETSCOUT InfiniStream - Subscription license + 1 year warranty support -1 license	2	USD 1.158.684,95	0%	30%	USD 347.605,49	USD 1.506.290,44	R$ 8.194.219,97
Não Encontrado	7	Licenciamento avançado de análise de aplicações, com 36 (trinta e seis) meses de subscrição e garantia oficial da fabricante	-	-	2	USD -	0%	30%	USD -	USD -	R$ -
Não Encontrado	8	Licenciamento avançado de análise de análise de metadados, com 36 (trinta e seis) meses de subscrição e garantia oficial da fabricante	-	-	2	USD -	0%	30%	USD -	USD -	R$ -
https://estore.accunetsolutions.com	9	Módulo de expansão do processamento, com 36 (trinta e seis) meses de garantia oficial da fabricante	D-02725-XSJA1	NetScout nGenius Decryption Appliance nDA-2725 - decryption appliance	2	USD 81.456,99	70%	0%	USD 57.019,89	USD 138.476,88	R$ 753.314,24
Não Encontrado	10	Módulo de expansão para a captura do tráfego “inline”, com 36 (trinta e seis) meses de garantia oficial da fabricante	-	-	2	0	70%	0%	USD -	USD -	R$ -
https://www.shi.com	11	Licenciamento para o gerenciamento centralizado da solução, com 36 (trinta e	91FV0L	nGeniusOne - License	2	USD 29.299,00	0%	30%	USD 8.789,70	USD 38.088,70	R$ 207.202,53

		seis) meses de garantia oficial da fabricante									
Não Encontrado	12	Interceptador do tráfego virtualizado avançado, com 36 (trinta e seis) meses de garantia oficial da fabricante	-	-	1	USD -	0%	30%	USD -	USD -	R$ -
https://www.cdw.com	13	Chassi para interconector passivo de interceptação do tráfego - interfaces ópticas	340-1080	NetScout HD Fiber TAP - tap splitter - 1GbE, 10GbE, 40GbE, 100GbE, 25GbE	1	USD 333,99	70%	0%	USD 233,79	USD 567,78	R$ 3.088,74
Não Encontrado	14	Interconector passivo de interceptação do tráfego – interfaces SFP	-	-	4	USD -	70%	0%	USD -	USD -	R$ -
Não Encontrado	15	Interconector passivo de interceptação do tráfego – interfaces QSFP	-	-	4	USD -	70%	0%	USD -	USD -	R$ -
Não Encontrado	16	Interconector passivo de interceptação do tráfego – interfaces RJ-45	-	-	4	USD -	70%	0%	USD -	USD -	R$ -
Não Encontrado	17	Concentrador de Tráfego de Segurança, com 36 (trinta e seis) meses de garantia oficial da fabricante	-	-	4	USD -	70%	0%	USD -	USD -	R$ -
https://texas.gs.shi.com	18	Transceiver tipo 1 – 1 Gbps ethernet	321-2313	NetScout - SFP (mini-GBIC) transceiver module	1	USD 506,00	70%	0%	USD 354,20	USD 860,20	R$ 4.679,49
https://www.cdw.com	19	Transceiver tipo 2 – 10 Gbps ethernet	321-2185	SFP+ Transceiver Module (10GbE, 10GBase-SR,	8	USD 1.667,99	70%	0%	USD 1.167,59	USD 2.835,58	R$ 15.425,57

				10GBase-SX, LC MM)							
Kromos Conexões	20	Transceiver tipo 3 – 25 Gbps ethernet	-	Compatible TAA Compliant 25GBase-SR SFP28 Transceiver (MMF, 850nm, 100m, LC, DOM)	8	-	-	-	-	-	R$ 2.490,00
TELLYCOM	21	Transceiver tipo 4 – 100 Gbps ethernet	N/A	100gbase-ezr4 qsfp28, 1310nm lwdm 100km smf, soa, lc ddm duplex, transceptor óptico miljet	8	-	-	-	-	-	R$ 11.186,00

PESQUISA NO CATÁLOGO DA SOLUÇÃO GIGAMON											
CATÁLOGO	**ITEM**	**DESCRIÇÃO**	**SKU**	**DESCRIÇÃO**	**QTD**	**UNITÁRIO**	**IMPOSTO TOTAL DE IMPORTAÇÃO DE HARDWARE (PJ)**	**IMPOSTO TOTAL DE IMPORTAÇÃO DE SOFTWARE (PJ)**	**CUSTO COM IMPORTAÇÃO**	**CUSTO UNITÁRIO TOTAL**	**CUSTO UNITÁRIO EM MOEDA NACIONAL**
https://irp.cdn-website.com	4	Equipamento para a interceptação do tráfego, com 36 (trinta e seis) meses de garantia oficial da fabricante	GVS-HC2A1	GigaVUE-HC2 base unit w/ chassis, Control Card Version 2, 1 Fan Tray, CLI, 2 power supplies, AC power	2	USD 29.995,00	70%	0%	USD 20.996,50	USD 50.991,50	R$ 277.393,76
https://irp.cdn-website.com			SMT-HC0-R	GigaSMART, GigaVUE-HC2 rear module (includes Slicing, Masking, Source Port & GigaVUE Tunneling De-	2	USD 24.000,00	0%	30%	USD 7.200,00	USD 31.200,00	R$ 169.728,00

				Encapsulation SW)							
https://irp.cdn-website.com	5	Licenciamento de desduplicação do tráfego, com 36 (trinta e seis) meses de subscrição e garantia oficial da fabricante	SMT-HC0-DD1	GigaSMART, GigaVUE-HC2, De-Duplication feature license per GigaSMART module	2	USD 14.995,00	0%	30%	USD 4.498,50	USD 19.493,50	R$ 106.044,64
https://irp.cdn-website.com	6	Licenciamento avançado de descriptação do tráfego, com 36 (trinta e seis) meses de subscrição e garantia oficial da fabricante	SMT-HC0-INSSL	GigaSMART, GigaVUE-HC2, SSL Decryption for Inline and Out of Band Tools Feature License per GigaSMART module	2	USD 17.995,00	0%	30%	USD 5.398,50	USD 23.393,50	R$ 127.260,64
https://irp.cdn-website.com	7	Licenciamento avançado de análise de aplicações, com 36 (trinta e seis) meses de subscrição e garantia oficial da fabricante	SMT-HC0-ASF	GigaSMART, GigaVUE-HC2, Application Session Filtering feature license per GigaSMART module; requires SMT-HC0-APF	2	USD 9.995,00	0%	30%	USD 2.998,50	USD 12.993,50	R$ 70.684,64
https://irp.cdn-website.com	8	Licenciamento avançado de análise de análise de metadados, com 36 (trinta e seis) meses de subscrição e garantia oficial da fabricante	SMT-HC0-AMI	Application Metadata Intelligence (1 Month) – GigaVUE-HC2 (12-Month Minimum) *Includes bundled Elite Support	2	USD 46.620,00	0%	30%	USD 13.986,00	USD 60.606,00	R$ 329.696,64
https://irp.cdn-website.com	9	Módulo de expansão do processamento, com 36 (trinta e seis) meses de garantia oficial da fabricante	SMT-HC0-X16	GigaSMART, GigaVUE-HC2, Front Module, 16 10G cages (includes Slicing, Masking, Source Port & GigaVUE Tunneling De-	2	USD 28.995,00	70%	0%	USD 20.296,50	USD 49.291,50	R$ 268.145,76

				Encapsulation SW)							
https://irp.cdn-website.com	10	Módulo de expansão para a captura do tráfego “inline”, com 36 (trinta e seis) meses de garantia oficial da fabricante	BPS-HC0-D25A4G	Bypass Combo Module, GigaVUE-HC2, 4 SX/SR 50/125 BPS pairs, 16 10G cages	2	USD 29.995,00	70%	0%	USD 20.996,50	USD 50.991,50	R$ 277.393,76
https://www.gigamon.com	11	Licenciamento para o gerenciamento centralizado da solução, com 36 (trinta e seis) meses de garantia oficial da fabricante	GFM-FM000-SW-TM	Monthly term license for GigaVUE-FM Prime Edition, manage up to 1,000 Physical Visibility Fabric Nodes. Includes Bundled Elite-Plus Software Support.	1	USD 79.200,00	0%	30%	USD 23.760,00	USD 102.960,00	R$ 560.102,40
https://www.gigamon.com	12	Interceptador do tráfego virtualizado avançado, com 36 (trinta e seis) meses de garantia oficial da fabricante	VBL-50T-BN-CORE	Monthly Term license for CoreVUE software up to 50TB/Day for cloud and virtual env. Capabilities include: Advanced Tunneling, Slicing, Masking, Advanced Load Balancing. Includes Bundled Elite-Plus Software Support.	1	USD 124.740,00	0%	30%	USD 37.422,00	USD 162.162,00	R$ 882.161,28
https://irp.cdn-website.com	13	Chassi para interconector passivo de interceptação do tráfego - interfaces ópticas	TAP-M200	G-TAP M Series 1 RU chassis. Supports up to 6 M Series TAP modules	1	USD 495,00	70%	0%	USD 346,50	USD 841,50	R$ 4.577,76

https://irp.cdn-website.com	14	Interconector passivo de interceptação do tráfego – interfaces SFP	TAP-252	Dual optical GigaTAP module, 50/50 Multimode, 850nm, 62.5/125 micron fiber, requires TAP-200 chassis, 1/10G	1	USD 1.095,00	70%	0%	USD 766,50	USD 1.861,50	R$ 10.126,56
https://irp.cdn-website.com	15	Interconector passivo de interceptação do tráfego – interfaces QSFP	TAP-M453	G-TAP M Series 40/100Gb TAP module, 50/50 Singlemode, taps 6 40/100G LR4 links, requires TAP-M200 chassis	1	USD 4.495,00	70%	0%	USD 3.146,50	USD 7.641,50	R$ 41.569,76
https://irp.cdn-website.com	16	Interconector passivo de interceptação do tráfego – interfaces RJ-45	GTP-ATX01	G-TAP A Series, Always On copper TAP, AC Power (US Plug)	1	USD 1.495,00	70%	0%	USD 1.046,50	USD 2.541,50	R$ 13.825,76
https://irp.cdn-website.com	17	Concentrador de Tráfego de Segurança, com 36 (trinta e seis) meses de garantia oficial da fabricante	GVS-TAC21	GigaVUE-TA200 edge node, 32 100G ports enabled, 2 power supplies, 4 fan trays, AC power	1	USD 34.995,00	70%	0%	USD 24.496,50	USD 59.491,50	R$ 323.633,76
https://irp.cdn-website.com	18	Transceiver tipo 1 – 1 Gbps ethernet	SFP-501	1G SFP, Copper, UTP with RJ45 interface. Not TAA Compliant.	8	USD 205,00	70%	0%	USD 143,50	USD 348,50	R$ 1.895,84
https://www.gigamon.com	19	Transceiver tipo 2 – 10 Gbps ethernet	SFP-532	10G SFP+, Multimode SR. Not TAA Compliant.	8	USD 835,00	70%	0%	USD 584,50	USD 1.419,50	R$ 7.722,08
https://www.gigamon.com	20	Transceiver tipo 3 – 25 Gbps ethernet	SFP-552	25G SFP28, Multimode SR. Not TAA Compliant.	8	USD 835,00	70%	0%	USD 584,50	USD 1.419,50	R$ 7.722,08
https://www.gigamon.com	21	Transceiver tipo 4 – 100 Gbps ethernet	Q28-508	100G QSFP28, Multimode SWDM4. Not	8	USD 2.995,00	70%	0%	USD 2.096,50	USD 5.091,50	R$ 27.697,76

				TAA Compliant.							

6.4.6. Esclarecemos a seguir o valor total estimado, com base nas referências identificadas em domínios públicos na web, de 2 (duas) fabricantes analisadas:

6.4.6.1. NetScout: R$ 19.507.590,94 (unitários multiplicados pelas quantidades estimadas);

6.4.6.2. Gigamon: R$ 5.659.294,56 (unitários multiplicados pelas quantidades estimadas).

6.4.6.3. Os percentuais de impostos totais representam uma estimativa com base nas tributações comuns de importação de mercadorias e serviços, vide pesquisa feita na legislação nacional e nas modalidades de cálculo tributário.

6.4.6.4. A tributação de mercadoria (hardware) soma tributos como Imposto de Importação, IPI, PIS, COFINS e ICMS (movimentação de mercadoria para o estado do Rio de Janeiro).

6.4.6.5. A tributação de importação de software soma tributos como ISS, IRRF, CIDE, PIS, COFINS e CSLL.

6.4.6.6. A taxa cambial empregada foi de R$ 5,449 por USD 1,00;

6.4.6.7. Os percentuais de tributação, médios, foram estipulados com base nas legislações:

6.4.6.8. Decreto nº 6.759/2009, o qual "Regulamenta a administração das atividades aduaneiras, e a fiscalização, o controle e a tributação das operações de comércio exterior".

6.4.6.9. Decreto nº 7.212/2010, o qual "Regulamenta a cobrança, fiscalização, arrecadação e administração do Imposto sobre Produtos Industrializados – IPI".

6.4.6.10. Lei Federal 10.865/2004, a qual "Dispõe sobre a Contribuição para os Programas de Integração Social e de Formação do Patrimônio do Servidor Público e a Contribuição para o Financiamento da Seguridade Social incidentes sobre a importação de bens e serviços e dá outras providências".

6.4.6.11. Lei Complementar 87/1996, a qual "Dispõe sobre o imposto dos Estados e do Distrito Federal sobre operações relativas à circulação de mercadorias e sobre prestações de serviços de transporte interestadual e intermunicipal e de comunicação, e dá outras providências. (LEI KANDIR)".

6.4.6.12. Lei Complementar 116/2003, a qual "Dispõe sobre o Imposto Sobre Serviços de Qualquer Natureza, de competência dos Municípios e do Distrito Federal, e dá outras providências".

6.4.6.13. Lei 9.779/1999, a qual "Altera a legislação do Imposto sobre a Renda, relativamente à tributação dos Fundos de Investimento Imobiliário e dos rendimentos auferidos em aplicação ou operação financeira de renda fixa ou variável, ao Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e das Empresas de Pequeno Porte - SIMPLES, à incidência sobre rendimentos de beneficiários no exterior, bem assim a legislação do Imposto sobre Produtos Industrializados - IPI, relativamente ao aproveitamento de créditos e à equiparação de atacadista a estabelecimento industrial, do Imposto sobre Operações de Crédito, Câmbio e Seguros ou Relativas a Títulos e Valores Mobiliários - IOF, relativamente às operações de mútuo, e da Contribuição Social sobre o Lucro Líquido, relativamente às despesas financeiras, e dá outras providências".

6.4.7. A mensuração visa a determinação de um valor de referência e da possibilidade de obtenção dos bens previstos, entretanto, a análise **requer uma apuração minuciosa** sobre os reais valores praticados de mercado na aquisição desse tipo de solução.

6.4.8. Em nossas pesquisas, **não fora possível identificar** os seguintes parâmetros:

6.4.9. Se todos os valores apurados correspondem a oferta correta das fabricantes;

6.4.9.1. Se os valores de licenciamento e suporte estão inclusos corretamente nos itens da oferta;

6.4.9.2. Por exemplo, fora identificado valor de suporte para algumas licenças, mas não o seu custo correlato de licenciamento;

6.4.9.3. De modo análogo, para outros itens fora identificado o valor da licença, mas não do suporte correlato.

6.4.9.4. Se os itens identificados representam de modo fidedigno a oferta mais atual da fabricante analisada, sem qualquer peça ou componente que seja necessário para que a solução seja coesa.

6.4.9.5. Nesse diapasão, **sugere-se a correta apuração dos valores através de propostas oficiais de mercado**, evitando assim o abandono ou a inexequibilidade dos valores estimados da contratação.

6.4.9.6. Se ressalta que a análise anterior não pondera as possíveis cadeias de operações comerciais, o que impacta diretamente na formação correta dos tributos nacionais que incidem sobre a compra de mercadorias e serviços.

6.4.9.7. Frisa-se que a coleta de propostas para o processo deverá ser executada com o viés de garantir a aferição correta dos preços de mercado.

DESCRIÇÃO SUCINTA	QTDE	PREÇO UNITARIO	PREÇO MÉDIO UNITÁRIO	PREÇO GLOBAL
Equipamento para a interceptação do tráfego, com 36 (trinta e seis) meses de garantia oficial da fabricante	2	R$ 382.830,21 R$ 277.393,76	R$ 276.650,66	**R$ 553.301,32**

		R$ 169.728,00		
Licenciamento de desduplicação do tráfego, com 36 (trinta e seis) meses de subscrição e garantia oficial da fabricante	2	R$ 131.998,53 R$ 106.044,64	R$ 119.021,58	**R$ 238.043,16**
Licenciamento avançado de descriptação do tráfego, com 36 (trinta e seis) meses de subscrição e garantia oficial da fabricante	2	R$ 8.194.219,97 R$ 127.260,64	R$ 4.160.740,30	**R$ 8.231.480,60**
Licenciamento avançado de análise de aplicações, com 36 (trinta e seis) meses de subscrição e garantia oficial da fabricante	2	R$ 70.684,64	R$ 70.684,64	**R$ 141.369,28**
Licenciamento avançado de análise de análise de metadados, com 36 (trinta e seis) meses de subscrição e garantia oficial da fabricante	2	R$ 329.696,64	R$ 329.696,64	**R$ 659.393,28**
Módulo de expansão do processamento, com 36 (trinta e seis) meses de garantia oficial da fabricante	2	R$ 753.314,24 R$ 268.145,76	R$510.730,00	**R$ 1.021.460,00**
Módulo de expansão para a captura do tráfego “inline”, com 36 (trinta e seis) meses de garantia oficial da fabricante	2	R$ 277.393,76	R$ 277.393,76	**R$ 554.787,52**
Licenciamento para o gerenciamento centralizado da solução, com 36 (trinta e seis) meses de garantia oficial da fabricante	2	R$ 207.202,53 R$ 560.102,40	R$ 383.652,46	**R$ 767.304,92**
Interceptador do tráfego virtualizado avançado, com 36 (trinta e seis) meses de garantia oficial da fabricante	1	R$ 882.161,28	R$ 882.161,28	**R$ 882.161,28**
Chassi para interconector passivo de interceptação do tráfego - interfaces ópticas	4	R$ 3.088,74 R$ 4.577,76	R$ 3.833,25	**R$ 15.333,00**
Interconector passivo de interceptação do tráfego – interfaces SFP	4	R$ 10.126,56	R$ 10.126,56	**R$ 40.506,24**
Interconector passivo de interceptação do tráfego – interfaces QSFP	4	R$ 41.569,76	R$ 41.569,76	**R$ 166.279,04**
Interconector passivo de interceptação do tráfego – interfaces RJ-45	4	R$ 13.825,76	R$ 13.825,76	**R$ 55.303,04**
Concentrador de Tráfego de Segurança, com 36 (trinta e seis) meses de garantia oficial da fabricante	4	R$ 323.633,76	R$ 323.633,76	**R$ 1.294.535,04**
Transceiver tipo 1 – 1 Gbps ethernet	1	R$ 4.679,49 R$ 1.895,84	R$ 3.287,66	**R$ 26.301,28**

Transceiver tipo 2 – 10 Gbps ethernet	8	R$ 15.425,57 R$ 7.722,08	R$ 11.573,82	**R$ 92.590,56**
Transceiver tipo 3 – 25 Gbps ethernet	8	R$ 2.490,00 R$ 7.722,08	R$ 5.106,04	**R$ 40.848,32**
Transceiver tipo 4 – 100 Gbpsethernet	8	R$ 11.186,00 R$ 27.697,76	R$ 19.441,88	**R$ 155.535,04**

ÓRGÃO PÚBLICO	**DESCRIÇÃO SUCINTA**	**PREÇO UNITÁRIO**	**Atualização pelo ICTI * (7,10% - jan/25**	**QTD SOLICITADA**	**PREÇO GLOBAL**	**PREÇO MÉDIO GLOBAL**
Tribunal de Contas do Distrito Federal Pregão Eletrônico Nº 17/2023 110777934	Prestação de serviços técnicos especializados, sob demanda (por meio de Ordem de Serviço – O.S.), de acordo com catálogo de serviços	R$ 415,53	R$ 445,03	3.238	R$ 1.441.007,14	**R$ 1.379.960,05**
Departamento de policia federal 200342 - diretoria de tecn.da informação e inovação relação de itens - pregão eletrônico nº 90006/2024-000 srp 110777455	Serviço de suporte técnico especializado	R$ 398,25	R$ 426,52	3.238	R$ 1.381.071,76	
Tribunal de Contas do Município de São Paulo Pregão Eletrônico 14/2023 (itens 1,2 e 3) 110778270	Serviço Técnico Especializado em Horário Comercial (Banco de Horas), pelo período de 12 meses	R$ 380,00	R$ 406,98	3.238	R$ 1.317.801,24	

6.4.9.8. Face ao exposto, o PRODERJ observa as condições normativas para a construção do valor estimado da contratação, vide Lei Federal 14.133/2021.

"*Art. 23. O valor previamente estimado da contratação deverá ser compatível com os valores praticados pelo mercado, considerados os preços constantes de bancos de dados públicos e as quantidades a serem contratadas, observadas a potencial economia de escala e as peculiaridades do local de execução do objeto."*

"*IV - pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital;"*

Valor estimado Cenário 2 - Solução 2

Componentes de Hardware e Interceptação de Tráfego, Licenciamentos integrados e Serviço Técnico Especializado
R$ 16.316.492,97

6.5. **CENÁRIO 3 - Solução de gerenciamento e orquestração**

6.5.1. **Solução 1 - Contratações Similares - Elastic Cloud Enterprise - ECE**

ÓRGÃO PÚBLICO	CONTRATAÇÕES SIMILARES					
	DESCRIÇÃO SUCINTA	**QTDE**	**PREÇO UNITÁRIO**	**Atualização pelo ICTI * (7,10% - jan/25**	**PREÇO GLOBAL**	**PREÇO MÉDIO GLOBAL**
Departamento de policia federal 200342 - diretoria de tecn.da informação e inovação relação de itens - pregão eletrônico nº 90006/2024-000 srp 110777455	Subscrição anual de Licença de software Elastic Cloud Enterprise - ECE	24	R$ 101.538,61	R$ 108.747,85	R$ 2.609.948,40	**R$ 9.029.668,80**
Tribunal de Contas do Distrito Federal Pregão Eletrônico Nº 17/2023 110777934	Subscrição de licença de software Elastic Stack Enterprise, contemplando a última versão disponibilizada (lts), possuindo as funcionalidades Enterprise Search, Kibana e Security	24	R$ 601.050,00	R$ 643.724,55	R$ 15.449.389,20	
Departamento de policia federal 200342 - diretoria de tecn.da informação e inovação relação de itens - pregão eletrônico nº 90006/2024-000 srp 110777455	Serviço de suporte técnico especializado	5.082	R$ 398,25	R$ 426,52	R$ 2.167.574,64	**R$ 2.214.608,55**
Tribunal de Contas do Distrito Federal Pregão Eletrônico Nº 17/2023 110777934	Prestação de serviços técnicos especializados, sob demanda (por meio de Ordem de Serviço – O.S.), de acordo com catálogo de serviços	5.082	R$ 415,53	R$ 445,03	**R$ 2.261.642,46**	

6.5.1.1. O licenciamento Elastic Cloud Enterprise (ECE) está relacionado à **quantidade total de RAM que seus deployments do Elastic Stack consomem** dentro do ECE. capacidade de memória do PRODERJ é de 24GB.

Valor estimado Cenário 3 - Solução 1
Elastic Cloud Enterprise - ECE
R$ 11.244.277,35

6.5.2. **Solução 2 - Contratações Similares - software splunk enterprise; serviços profissionais especializados**

ÓRGÃO PÚBLICO	CONTRATAÇÕES SIMILARES					
	DESCRIÇÃO SUCINTA	**QTDE**	**PREÇO UNITÁRIO**	**Atualização pelo ICTI * (7,10% - jan/25**	**PREÇO GLOBAL**	**PREÇO MÉDIO GLOBAL**
Banco central do brasil Pregão 98/2021 https://portaldatransparencia.gov.br/licitacoes/984103834?ordenarPor=dataEmissao&direcao=asc 110780698	Cessão temporária de licenças, garantia e suporte técnico avançado do software splunk enterprise; serviços profissionais especializados splunk e serviços de manutenção da infraestrutura splunk do banco central, pelo período de 36 (tri nta e seis) meses.	24	R$ 436.250,00	R$ 467.223,75	R$ 11.213.370,00	
Ministério da Defesa Comando do Exército Base Administrativa so CCOMGEX PREGÃO ELETRÔNICO Nº 00016/2021-000 110777820	Contratação de renovação das licenças da solução de software Splunk Enterprise atualmente utilizada no CDCiber de 100GB/dia (cem gigabytes por dia), expansão da solução Splunk contendo o módulo UBA (User Behavior Analytics), treinamento técnico oficial, suporte técnico e garantia técnica por 36 meses.	24	R$ 1.863.333,33	R$ 1.995.630,00	R$ 47.895.120,00	**R$ 29.554.245,00**

6.5.2.1. O licenciamento **software splunk enterprise** geralmente está relacionado à **quantidade total de RAM** a capacidade de memória do PRODERJ é de 24 GB

Valor estimado Cenário - Solução 2

Software splunk enterprise; serviços profissionais especializados
R$ 29.554.245,00

6.6. **Custo de Propriedade**

CENÁRIO 1 - SOLUÇÃO 1 - NDR	**VALOR UNITÁRIO ESTIMADO**
Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, com instalação da Solução.	**R$ 2.007.328,06**
Serviço técnico especializado de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	**R$ 443.626,85**
Treinamento da Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	**R$ 62.242,50**

CENÁRIO 1 - SOLUÇÃO 2 - SOC	**VALOR UNITÁRIO ESTIMADO**
Contratação de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, baseado em serviço SOC-as-a-Service (Security Operations Center-as-a-Service).	**R$ 11.566.771,27**
Treinamento solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, baseado em serviço SOC-as-a-Service (Security Operations Center-as-a-Service).	**R$ 97.421,55**

CENÁRIO 2 - Infraestrutura de rede solução 1	**VALOR UNITÁRIO ESTIMADO**
Equipamento para a interceptação do tráfego com suporte técnico, Instalação e Configuração	**R$ 210.153,62 + R$ 22.807,58 = R$ 232.961,20**
Prestação de serviços técnicos especializados, sob demanda	**R$435,77**

CENÁRIO 2 Infraestrutura de rede solução 2	**VALOR UNITÁRIO ESTIMADO**
Componentes de Hardware e Interceptação de Tráfego, Licenciamentos integrados e Serviço Técnico Especializado	**R$ 14.936.532,92**
Serviço Técnico Especializado em Horário Comercial (Banco de Horas)	**R$ 426,18**

CENÁRIO 3 - Solução 1 Elastic	**VALOR MÉDIO UNITÁRIO ESTIMADO**

Subscrição de licença de software Elastic Stack Enterprise	**R$ 9.029.668,80**
Prestação de serviços técnicos especializados, sob demanda	**R$ 2.214.608,55**

CENÁRIO 3 - Solução 2 - splunk	**VALOR MÉDIO UNITÁRIO ESTIMADO**
Cessão temporária de licenças, garantia e suporte técnico avançado do software splunk	**R$ 29.554.245,00**

7. **MÉTRICA PARA MENSURAÇÃO DOS SERVIÇOS**

7.1. Para serviços especializados em implantação de soluções de NDR (Network Detection and Response), as métricas de remuneração variam conforme o grau de complexidade e escopo dos serviços. Algumas formas de medição são mais adequadas a esse tipo de contratação:

7.2. **Homem-Hora (H/H):**

7.2.1. Descrição: É a métrica mais comum e direta. O valor do serviço é calculado com base no número de horas trabalhadas pelos profissionais alocados no projeto (como analistas de segurança, engenheiros de redes, consultores especialistas na solução ofertada, etc.), multiplicadas por uma taxa horária conforme a senioridade de cada perfil.

7.2.2. Vantagens: Traz transparência ao processo, flexibilidade para ajustes de escopo ao longo do projeto e facilita o controle de esforço por parte do contratante.

7.2.3. Desvantagens: Pode gerar incertezas quanto ao custo final total, sendo necessário um acompanhamento rigoroso das horas alocadas e entregas parciais.

7.2.4. Aplicação na Consultoria: Muito utilizada nas etapas de levantamento técnico da rede, diagnóstico de maturidade em segurança, configuração e integração das ferramentas contratadas ao ambiente existente, capacitação das equipes, suporte técnico pós-implantação e ajustes finos de tuning e detecção.

7.2.5. Valor Fixo por Pacote/Fase (Escopo Fechado):

7.2.6. Descrição: A contratada propõe um valor fixo por fase da implantação da solução ofertada (ex: diagnóstico e mapeamento da infraestrutura de rede, implantação dos componentes da solução, integração com plataforma de observabilidade, configuração de políticas de detecção, treinamento de equipes).

7.2.7. Vantagens: Proporciona previsibilidade de custos para o contratante e estimula maior eficiência da contratada, que buscará concluir as fases no prazo e dentro do escopo.

7.2.8. Desvantagens: Requer escopos muito bem definidos previamente; eventuais mudanças ou ampliações podem exigir aditivos contratuais e ajustes de cronograma.

7.2.9. Aplicação na Consultoria: Indicada para fases com entregáveis bem tangíveis, como “Mapeamento de Fluxo de Rede com Identificação de Gaps”, “Implantação da solução e Integração com ferramental de observabilidade”, “Treinamento de Equipes SOC/NOC”, entre outras.

7.3. **Unidade de Serviço Técnico (UST):**

7.3.1. Descrição: Unidade padronizada de medição de esforço técnico utilizada por alguns órgãos públicos no Brasil. Cada UST representa um conjunto de atividades padronizadas, com valor unitário definido em tabela. A remuneração é calculada com base no número de USTs consumidas.

7.3.2. Vantagens: Facilita a padronização e a comparação entre propostas técnicas em processos licitatórios; oferece boa previsibilidade orçamentária quando as atividades são bem definidas.

7.3.3. Desvantagens: A definição precisa de USTs para atividades especializadas em cibersegurança e implantação das soluções pode ser difícil e, muitas vezes, não refletir adequadamente a complexidade e a variabilidade técnica do projeto.

7.3.4. Aplicação na Consultoria: Mais adequada para atividades rotineiras ou suporte técnico contínuo após a implantação da solução, como “Análise de Alertas das soluções ” ou “Ajustes em Regras de Detecção”, desde que padronizadas e quantificáveis.

7.4. **Pontos de Função (PF):**

7.4.1. Descrição: Métrica funcional utilizada para mensurar funcionalidades de sistemas de software do ponto de vista do usuário. Mede entregas funcionais de desenvolvimento, manutenção ou melhoria de sistemas.

7.4.2. Vantagens: É útil para remunerar funcionalidades entregues em projetos de software, pois foca no resultado funcional e não no tempo de execução.

7.4.3. Desvantagens: Não se aplica diretamente a serviços de consultoria técnica, estratégica ou de implantação de soluções de segurança como o NDR, que não envolvem desenvolvimento de sistemas sob medida com funcionalidades quantificáveis.

7.4.4. Aplicação na Consultoria: Inadequada para projetos de implantação de soluções NDR. Pode ser utilizada apenas em casos em que a contratação envolva desenvolvimento complementar de funcionalidades específicas ou customizações em sistemas correlatos (como SIEMs integrados ao NDR), desde que essas entregas sejam quantificáveis funcionalmente.

7.5. **Conclusão sobre a Métrica Preferencial:**

7.5.1. Considerando a natureza técnica e recorrente das atividades envolvidas na implantação das soluções previstas na contratação, a utilização da métrica de Unidade de Serviço Técnico (UST) apresenta-se como a mais vantajosa. A padronização proporcionada pelas USTs permite maior previsibilidade de custos e facilita a comparação entre propostas em processos licitatórios, além de estar alinhada com práticas comuns na administração pública. Quando bem definidas, as USTs permitem mensurar de forma objetiva etapas como instalação de sensores, configuração de regras de detecção, integração com sistemas legados (como SIEM ou firewalls), treinamentos operacionais e suporte técnico pós-implantação. Essa abordagem contribui para a transparência na contratação, a eficiência na execução e a rastreabilidade dos serviços prestados, especialmente em ambientes com múltiplas unidades organizacionais ou redes distribuídas.

7.6. **Utilização Periódica dos Serviços Técnicos Especializados**

7.6.1. A utilização dos serviços técnicos especializados sob demanda, ocorrerá de forma contínua e distribuída. Esta previsão é plenamente justificada pela necessidade de prover suporte técnico eficiente e especializado a um ambiente de grande porte. Trata-se de um cenário de alta complexidade, que demanda acompanhamento técnico permanente para garantir a estabilidade, a segurança e a eficiência da infraestrutura tecnológica.

7.6.2. As atividades previstas incluem instalação, configuração, atualização, ajustes, tuning, hardening, otimização de desempenho, configuração de segurança, personalizações e suporte a funcionalidades avançadas, entre outras. Todas essas ações possuem natureza recorrente e estão sujeitas a revisões periódicas, correções pontuais e melhorias contínuas, exigindo, portanto, a utilização mensal dos serviços contratados. Além disso, a possibilidade de inovações ou alterações no projeto original durante sua execução reforça a necessidade de assistência técnica contínua, de modo a assegurar a adequada adaptação da solução às novas demandas que possam surgir.

7.6.3. Ressalta-se ainda que parte dos serviços compreende atendimentos não cobertos pelo suporte técnico do fabricante da solução, voltados à exploração personalizada de todas as potencialidades dos softwares no ambiente da PRODERJ, o que demanda pronta disponibilidade e atuação regular da equipe de consultoria especializada.

8. **DEFESA DA MARCA**

8.1. Após análise apresentada no item "**LEVANTAMENTO DE MERCADO**" Estudo, optou-se pela escolha da marca, conforme motivos exposto abaixo:

8.1.1. Atualmente, o PRODERJ utiliza a versão gratuita do Elasticsearch. Essa ferramenta não só consolida eventos de segurança da informação (SIEM) para auxiliar na tomada de decisões, como também fornece outras informações valiosas para a rotina operacional do PRODERJ.

8.1.2. A escolha do **Licenciamento Elastic Enterprise On-Premises** para a solução de monitoramento de comportamento anômalo de rede, detecção e resposta a incidentes de segurança da informação, e interceptação de tráfego, conforme detalhado no no Estudo, é fundamentada em uma análise técnica e estratégica que visa garantir a máxima eficácia, escalabilidade, controle e conformidade para o ambiente da organização.

8.1.3. O Elastic Stack (composto por Elasticsearch, Kibana, Logstash, Beats, e outros componentes) é reconhecidamente uma plataforma líder de mercado para observabilidade, segurança e busca empresarial. A versão Enterprise On-Premises eleva essa capacidade, oferecendo um conjunto de funcionalidades e um modelo de implantação que se alinham perfeitamente às necessidades críticas de uma operação de segurança de grande porte.

8.1.4. Principais Justificativas para a Escolha:

- **Liderança de Mercado e Capacidade Comprovada:**
  - O Elastic Stack é amplamente reconhecido como líder em diversas áreas, incluindo **SIEM (Security Information and Event Management)** e **Observabilidade**, conforme atestado por relatórios de analistas da indústria. Essa liderança não se deve apenas à sua popularidade, mas à sua **capacidade técnica robusta** de ingestão e análise de dados em escala, essencial para o cenário de segurança que envolve grandes volumes de tráfego de rede e eventos.
  - A escolha de uma marca consolidada minimiza riscos de implementação e garante acesso a uma vasta comunidade de usuários, documentação e recursos de suporte.
- **Plataforma Unificada para Múltiplos Casos de Uso (SIEM e Observabilidade):**
  - O Elastic Enterprise On-Premises oferece uma **plataforma unificada** que integra funcionalidades de SIEM, observabilidade (logs, métricas, APM) e busca. Essa sinergia é vital para uma visão holística da segurança, permitindo a correlação de eventos de segurança com dados de desempenho e operacionais. Em um incidente, a capacidade de correlacionar informações de logs, métricas de rede e dados de interceptação de tráfego dentro de uma única plataforma acelera drasticamente a detecção, análise e resposta.
- **Controle Total e Soberania dos Dados com Implementação On-Premises:**
  - A opção **On-Premises** é crucial para organizações com **rigorosos requisitos de segurança, conformidade e soberania de dados**. Manter a infraestrutura e os dados dentro do próprio data center garante total controle sobre a segurança física e lógica, acesso aos dados e aderência a regulamentações locais (como LGPD) ou setoriais que proíbem ou restringem o armazenamento de dados sensíveis em nuvens públicas.

- Isso também permite otimizar a infraestrutura de hardware de acordo com as necessidades específicas de desempenho e custo da organização.

- **Escalabilidade Horizontal e Flexibilidade Arquitetural:**
  - O Elastic Stack é conhecido por sua **capacidade de escalabilidade horizontal**, permitindo o crescimento da capacidade de processamento e armazenamento adicionando mais nós à infraestrutura. O Licenciamento Enterprise On-Premises é projetado para suportar essas arquiteturas distribuídas, garantindo que a solução possa evoluir junto com o crescimento da rede e do volume de dados, sem a necessidade de reengenharia completa.
  - A flexibilidade para configurar a arquitetura (hot-warm, nodes dedicados, etc.) permite otimizar o desempenho e o custo de armazenamento para diferentes tipos de dados.
- **Recursos Avançados de Segurança e Análise (X-Pack Security, Machine Learning):**
  - A versão Enterprise habilita recursos avançados do Elastic Stack, incluindo o **X-Pack Security** (com controle de acesso baseado em função, autenticação LDAP/AD, criptografia) e **Machine Learning**. Esses recursos são indispensáveis para:
    - Proteger a própria plataforma de segurança.
    - Detectar padrões de comportamento anômalos e ameaças sofisticadas que não seriam identificadas por regras estáticas.
    - Reduzir falsos positivos e aumentar a eficácia da detecção.
- **Integração e Ecossistema:**
  - O Elastic Stack possui um rico ecossistema de integrações (Beats para coleta de dados, API para integração com outras ferramentas de segurança e ITOM) que facilitam a ingestão de dados de diversas fontes e a orquestração de respostas a incidentes. Essa capacidade de integração é fundamental para uma solução de segurança abrangente.

8.1.5. Ao optar pelo **Licenciamento Elastic Enterprise On-Premises**, a organização não está apenas adquirindo um software, mas uma **plataforma de segurança e observabilidade de ponta**, que oferece o controle, a performance e a escalabilidade necessários para proteger seus ativos mais valiosos em um ambiente dinâmico e complexo, alinhando-se com as diretrizes e necessidades técnicas do estudo preliminar.

9. JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO

9.1. **CENÁRIO 1 -** A decisão pela Solução 1, baseada em um appliance dedicado de Network Detection and Response (NDR), para atender às necessidades de segurança da CONTRATANTE, reflete uma análise aprofundada das opções disponíveis e a priorização de fatores críticos para um ambiente de missão crítica. Esta escolha se fundamenta na capacidade incomparável da Solução 1 de oferecer visibilidade em tempo real, análise comportamental avançada e controle total sobre os dados, elementos essenciais para uma postura de segurança robusta.

9.2. A Solução 1 se destaca por sua arquitetura de appliance dedicado, que garante alto desempenho e uma implantação simplificada. Sendo pré-configurada e otimizada, ela acelera o tempo de entrada em operação e minimiza os riscos de configurações inadequadas. Sua capacidade de atuar diretamente na infraestrutura da CONTRATANTE é crucial, proporcionando uma análise em tempo real de todo o tráfego de rede, impulsionada por inteligência artificial e machine learning. Isso permite identificar e responder rapidamente a comportamentos anômalos, ameaças desconhecidas (dia zero), movimentos laterais e atividades suspeitas, algo fundamental para a proteção proativa.

9.3. Outros pontos fortes da Solução 1 incluem a resposta automatizada a incidentes e a integração fluida com outras ferramentas de segurança (como EDRs e firewalls), criando um ecossistema de defesa mais coeso. O controle direto sobre a análise e o armazenamento de dados sensíveis no ambiente da organização é um diferencial significativo, garantindo suporte à conformidade com normativas de proteção de dados, como a LGPD. Embora represente um custo inicial mais elevado, este é visto como um investimento estratégico que se traduz em ganhos substanciais de confiabilidade, tempo de resposta e cobertura técnica, conforme atestado pelo benchmarking e pela presença de fornecedores líderes de mercado, como Darktrace, Vectra AI e ExtraHop.

9.4. Em contraste, as alternativas avaliadas apresentaram limitações importantes. A Solução 2 (SOC como Serviço), apesar de vantagens como baixo custo inicial e escalabilidade, foi desconsiderada devido à dependência de conectividade constante com a internet, latência na análise de dados em nuvem e restrições no controle direto sobre dados sensíveis. Essas desvantagens, somadas a desafios regulatórios e limitações na inspeção de tráfego criptografado, tornam-na inadequada para a rede de missão crítica da CONTRATANTE. A Solução 3 (software livre) foi tecnicamente inviável, carecendo de maturidade tecnológica, suporte contínuo, cobertura abrangente contra malwares e mecanismos de resposta automatizados. Além disso, os custos de implantação e a necessidade de investimentos em infraestrutura anularam a suposta economia inicial, introduzindo riscos inaceitáveis de manutenção e desempenho.

9.5. **CENÁRIO 2** - A escolha da Solução 2, Componentes de Hardware e Interceptação de Tráfego e Licenciamentos integrados, é a decisão mais estratégica e eficiente para a CONTRATANTE, baseada em uma análise comparativa aprofundada das abordagens disponíveis. Esta opção se destaca por sua capacidade de oferecer uma visão de segurança unificada, otimizada e com controle superior, atributos essenciais para um ambiente de rede complexo e que demanda alta performance.

9.5.1. A principal vantagem da Solução 2 reside em sua abordagem "turn-key" e unificada. Hardware e software vêm do mesmo ecossistema, garantindo compatibilidade máxima e otimização de desempenho. Isso se traduz em um aparelho dedicado projetado especificamente para a tarefa de interceptação e análise de tráfego, o que é crucial para alcançar alta performance e integração nativa. Licenciamentos para desduplicação, descriptografia avançada, análise de aplicações e análise de metadados são integrados a plataforma, otimizando o processamento e a capacidade de inspeção profunda de tráfego criptografado e de contextualização de aplicações. Essa integração facilita a detecção de ameaças que se escondem em tráfegos cifrados ou que se manifestam através de comportamentos anômalos de aplicações.

9.5.2. Além disso, a Solução 2 oferece um módulo de expansão de processamento específico do fornecedor, otimizado para o software, e um módulo para captura "inline" que habilita capacidades diretas interceptação do tráfego de modo resiliente a falhas. O gerenciamento centralizado é simplificado através de uma console unificada, que gerencia toda plataforma do mesmo fornecedor, reduzindo a complexidade

operacional. Para ambientes modernizados, o software ou appliance virtualizado do fornecedor garante visibilidade nativa em tráfegos virtuais e na nuvem. A conectividade física utiliza componentes otimizados para o appliance, e o concentrador de tráfego de segurança é um appliance dedicado, otimizado para a consolidação de tráfego em infraestruturas apartadas, garantindo eficiência e desempenho. Por fim, o serviço técnico especializado é fornecido pelo próprio fornecedor ou por parceiros, garantindo expertise aprofundada na solução integrada.

9.5.3. Em contraste, a Solução 1, que apresenta teor simplificado na coleta de tráfego, sem a habilidade de interceptar granularmente as informações e, por conseguinte, prover uma análise holística quanto ao bloqueio ou a transmissão de dados para as ferramentas de segurança da informação. Tendo em vista que a solução não possui cunho abrangente e nem integrado de atuação, ela não adereça corretamente o ambiente do PRODERJ.

9.5.4. Portanto, para a CONTRATANTE, a Solução 2 representa a escolha superior e adequada ao contexto da contratação, mesmo em uma análise dos distintos lotes. Ela entrega uma plataforma coesa e otimizada, minimizando a complexidade operacional, garantindo alta performance e eficácia na interceptação do tráfego, e consolidando o suporte, o que é crucial para a segurança de uma rede de missão crítica.

9.6. **CENÁRIO 3 -** A escolha pela **Solução 1, baseada no Elastic Cloud Enterprise (ECE)**, para o tratamento e análise de dados operacionais, observabilidade, segurança da informação e busca empresarial, é justificada por sua superioridade técnica e estratégica, especialmente em um contexto que exige alto controle, flexibilidade e previsibilidade de custos.

9.6.1. O Elastic Cloud Enterprise (ECE) se destaca como uma plataforma robusta de orquestração e gerenciamento centralizado do Elastic Stack. Sua capacidade de implantar, escalar e administrar múltiplos clusters Elastic em qualquer infraestrutura (local, nuvem privada ou híbrida) com alto grau de automação e controle é um diferencial crucial. Isso permite à CONTRATANTE a manutenção do domínio direto sobre seus dados, um requisito fundamental para atender a requisitos de soberania, sigilo e conformidade regulatória, como a LGPD. A flexibilidade de implantação do ECE também possibilita o reaproveitamento de investimentos prévios em hardware e virtualização, otimizando recursos existentes.

9.6.2. Do ponto de vista técnico, a Solução 1 oferece vantagens inegáveis:

- Maior controle da infraestrutura e dos dados: Facilita a adesão a normas e a gestão da privacidade.
- Flexibilidade de implantação: Permite o uso em servidores existentes ou ambientes híbridos, otimizando investimentos.
- Isolamento de ambientes (multitenancy): Suporta múltiplos clusters independentes, adequados para atender diferentes áreas ou órgãos com distintas necessidades de segurança e recursos.
- Custo previsível: Baseado em recursos provisionados, e não em volume de ingestão, o que é financeiramente mais vantajoso para cargas de trabalho contínuas e pesadas, típicas de ambientes governamentais ou de grande porte.
- Acesso nativo a recursos avançados do Elastic Stack: Inclui detecção automatizada de anomalias, análise de logs e métricas, APM distribuído e recursos de SIEM, fornecendo uma suíte completa de funcionalidades de ponta.
- Interface unificada e APIs para automação: Reduz drasticamente a complexidade de gerenciamento operacional em larga escala.

9.6.3. Em contrapartida, a Solução 2 – Splunk Enterprise, apesar de ser uma ferramenta poderosa para análise de dados de máquina e ter forte atuação em observabilidade e segurança da informação, apresenta um modelo de licenciamento baseado em volume diário de ingestão de dados. Para cenários com grande volume de eventos contínuos, isso pode tornar sua adoção financeiramente inviável. Além disso, a instalação, operação e manutenção do Splunk exigem conhecimento técnico especializado e investimento contínuo em serviços profissionais, o que pode gerar gargalos operacionais e financeiros.

9.6.4. Portanto, a **Solução 1 (Elastic Cloud Enterprise - ECE)** é a escolha mais aderente às necessidades da CONTRATANTE, oferecendo uma plataforma robusta, controlável, flexível e com um modelo de custo mais previsível, garantindo a eficácia no tratamento e análise de grandes volumes de dados.

9.6.5. Desta forma a escolha da solução tomando como base os cenários analisados ficou da seguinte forma:

a) Cenário 1 - **Solução 1 - NDR (Network Detection and Response) integrada do fornecedor**

b) Cenário 2 - **Solução 2 - Componentes de Hardware e Interceptação de Tráfego e Licenciamentos integrados.**

c) Cenário 3 - **Solução 1 - baseada no Elastic Cloud Enterprise (ECE)**

10. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERANDO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

10.1. Trata-se de Contratação de empresa especializada na aquisição de solução de interceptação de tráfego, monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, com Instalação da Solução, incluindo hardware, software e demais componentes, bem como serviços de treinamento e garantia com manutenção do fabricante por 36 (trinta e seis) meses.

10.2. A descrição pormenorizada, considerando todo o ciclo de vida do objeto a ser contratado, de forma precisa, suficiente e clara, por meio de especificações técnicas ou de desempenho do objeto usuais de mercado, vedando-se aquelas que, por excessivas, irrelevantes ou desnecessárias, limitem a competição, estão descritas no ANEXO I - ESPECIFICAÇÃO TÉCNICA, deste documento.

10.3. O ciclo de vida deste objeto refere-se ao fato de que a expectativa de tempo de utilização ou validade da solução será de, no mínimo, 3 (três) anos que é o tempo de garantia do fabricante, ao qual está contemplado todo o suporte tecnológico, reposição de peças e atualizações de softwares internos. Pela sua natureza, a solução em appliances tem caráter definitivo, onde não se vislumbra no contexto atual nenhum fato que poderá causar a descontinuidade do uso da ferramenta, pelo contrário, pois a proteção contra ataques é uma necessidade essencial e permanente, visando a proteção integral dos dados, informações e dos sistemas custodiados pelo CONTRATANTE. Somente o treinamento que possui uma natureza distinta, por se tratar de um serviço a ser executado sob demanda, ao qual não se aplica análise de ciclo de vida.

10.4. **Características Gerais**

10.4.1. Deverá, obrigatoriamente, atender as especificações mínimas previstas neste documento, e seus Anexos, quanto às funcionalidades, integrações e compatibilidades com o ambiente físico e virtualizado do PRODERJ e demais Órgãos participantes.

10.4.2. Todas as capacidades foram especificadas em seu requisito mínimo, sempre podendo ser entregue capacidade superior.

11. ESTIMATIVA DAS QUANTIDADES

11.1. A definição precisa do quantitativo necessário para a contratação está intrinsecamente ligada aos resultados e conclusões do Estudo Técnico Preliminar (ETP). A elaboração do ETP é essencial para determinar as especificações técnicas, a viabilidade e a melhor solução para atender à demanda, o que, por sua vez, impactará diretamente na quantidade de bens ou serviços a serem contratados. Portanto, a definição do quantitativo será realizada após a conclusão da **Intenção de Registro de Preço (IRP)**, garantindo a precisão e a adequação da contratação às necessidades da administração pública.

Solução de interceptação de tráfego, monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, incluindo hardware, software e demais componentes, bem como treinamento e garantia com manutenção do fabricante por 36 (trinta e seis) meses.						
LOTE I						
ITEM	**ID SIGA**	**ID PCA**	**DESCRIÇÃO**	**MÉTRICA**	**FORMA DE FORNECIMENTO**	**QUANTIDADE ESTIMADA**
1	195087	15918	Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, com Instalação da Solução.	Unidade	Aquisição	02
2	195079	15932	Serviço técnico especializado de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	UST	Sob Demanda	6.080
3	195078	15931	Treinamento da Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	Turma	Sob Demanda	01
LOTE II						
4	196478	15936	Equipamento para a interceptação do tráfego	Unidade	Aquisição de Equipamento	02
5	195071	15921	Licenciamento de desduplicação do tráfego.	Unidade	Subscrição de Licença por 36 meses	02
6	195072	15923	Licenciamento avançado de descriptação do tráfego.	Unidade	Subscrição de Licença por 36 meses	02
7	195073	15927	Licenciamento avançado de análise de aplicações.	Unidade	Subscrição de Licença por 36 meses	02
8	195074	15935	Licenciamento avançado de análise de metadados.	Unidade	Subscrição de Licença por 36 meses	02
9	193207	15937	Módulo de expansão do processamento.	Unidade	Aquisição de Equipamento	02
10	123672	15933	Módulo de expansão para a captura do tráfego “inline”.	Unidade	Aquisição de Equipamento	02
11	195075	15924	Licenciamento para o gerenciamento centralizado da solução.	Unidade	Subscrição de Licença por 36 meses	01

12	195076	15938	Interceptador do tráfego virtualizado avançado.	Unidade	Subscrição de Licença por 36 meses	01
13	196651	15919	Chassi para interconector passivo de interceptação do tráfego - interfaces ópticas	Unidade	Aquisição de Equipamento	04
14	196668	15928	Interconector passivo de interceptação do tráfego – interfaces SFP	Unidade	Aquisição de Equipamento	04
15	196641	15925	Interconector passivo de interceptação do tráfego – interfaces QSFP	Unidade	Aquisição de Equipamento	04
16	196667	15916	Interconector passivo de interceptação do tráfego – interfaces RJ-45	Unidade	Aquisição de Equipamento	04
17	196499	15922	Concentrador de Tráfego de Segurança.	Unidade	Aquisição de Equipamento	01
18	195083	15915	Transceiver tipo 1 – 1 Gbps ethernet	Unidade	Aquisição de Equipamento	08
19	195084	15934	Transceiver tipo 2 – 10 Gbps ethernet	Unidade	Aquisição de Equipamento	08
20	195085	15926	Transceiver tipo 3 – 25 Gbps ethernet	Unidade	Aquisição de Equipamento	08
21	195086	15930	Transceiver tipo 4 – 100 Gbps ethernet	Unidade	Aquisição de Equipamento	08
22	196666	15929	Serviço técnico especializado para a solução de interceptação de tráfego.	UST	Sob Demanda	3.238
LOTE III						
23	195077	15917	Licenciamento Elastic Enterprise On-Premises.	Unidade	Subscrição de Licença por 36 meses	24
24	195080	15920	Serviço técnico especializado para o Licenciamento Elastic Enterprise On-Premises.	UST	Sob Demanda	5.082

11.2. Os **Itens de 1 a 3 do Lote I -** A lista detalhada dos itens acima incluem não apenas o software principal de NDR ("Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação"), mas também todos os componentes físicos, lógicos e de serviço necessários para a sua implementação e operação eficaz.

11.2.1. Os **Itens de 4 a 22 do Lote II -** A lista detalhada dos itens acima incluem não apenas o equipamento principal de interceptação de tráfego, mas também todos os componentes físicos, lógicos e de serviço necessários para a sua implementação e operação eficaz,tais como:

- **Hardware para interceptação e agregação de tráfego:** Equipamentos para interceptação do tráfego (TAPs passivos, concentradores de tráfego de segurança), módulos de expansão e transceivers de diversas velocidades. Isso é essencial para que a solução de interceptação possa "enxergar" todo o tráfego da rede.
- **Licenciamento avançado para análise de tráfego:** Desduplicação, descriptografia, análise de aplicações e metadados. Isso garante que a solução de interceptação possa processar o tráfego de forma eficiente e profunda, mesmo quando criptografado ou com alto volume.
- **Gerenciamento centralizado:** Licenciamento para gerenciar a solução de forma unificada.
- **Serviços e treinamento:** Instalação, treinamento e serviço técnico especializado para garantir que a solução seja corretamente implementada, configurada e operada pela equipe responsável.

11.3. **Item 1 do Lote I - Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, com Instalação da Solução.**

11.3.1. Esta solução é como um "segurança" que vigia constantemente o tráfego da sua rede de computadores. Em vez de procurar por ameaças já conhecidas (como um vírus específico), ela foca em detectar comportamentos incomuns ou inesperados. A inteligência e as funcionalidades principais dessa solução são baseadas em software. No entanto, para que esse software possa coletar os dados, processá-los e responder eficazmente, ele frequentemente depende de hardware (servidores, appliances dedicados e/ou sensores de rede) para sua execução e coleta de informações.

11.3.1.1. **Como funciona e para que serve:**

- Monitoramento e Detecção de Anomalias: A solução primeiro aprende o que é o "normal" na sua rede – quem se comunica com quem, qual o volume de dados, quais tipos de arquivos são acessados, etc. Se, de repente, um computador começa a enviar muitos dados para fora da rede em um horário estranho, ou um usuário acessa arquivos que nunca acessou antes, isso é considerado uma anomalia. **Isso pode indicar:**
    - Intrusões: Alguém não autorizado tentando acessar sua rede.
    - Malware: Vírus ou outros softwares maliciosos agindo silenciosamente.
    - Ataques internos: Um funcionário mal-intencionado tentando roubar dados.
    - Vazamento de dados: Informações sensíveis sendo enviadas para fora da rede sem permissão.
- **Análise de Incidentes**: Uma vez que uma anomalia é detectada, a solução não para por aí. Ela ajuda a analisar o incidente, fornecendo informações detalhadas sobre o que aconteceu, quando, onde e quem foi envolvido. Isso permite que a equipe de segurança entenda a gravidade da ameaça e seu possível impacto.
- **Resposta a Incidentes:** Finalmente, a solução auxilia na resposta ao incidente. Isso pode envolver:
    - Isolamento: Desconectar o dispositivo infectado para evitar que o problema se espalhe.
    - Bloqueio: Impedir que o ataque continue ou que dados sejam vazados.
    - Investigação: Coletar evidências para entender a causa raiz e evitar futuros ataques.
    - Contenção: Limitar os danos causados pelo incidente.

11.3.1.2. **SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO E IMPLEMENTAÇÃO**

11.3.1.3. Basicamente, o serviço de instalação pega a ferramenta de monitoramento de comportamento anômalo e a coloca para funcionar na sua rede. Isso inclui:

- **Planejamento:** Entender a sua rede, seus sistemas e suas necessidades de segurança.
- **Instalação:** Fazer a instalação física ou virtual dos componentes da solução nos seus servidores e equipamentos de rede.
- **Configuração:** Ajustar a solução para que ela aprenda o "normal" da sua rede, defina as regras de detecção de anomalias e se integre com outros sistemas de segurança que você já tenha.
- **Testes:** Garantir que tudo está funcionando corretamente, detectando as anomalias e gerando os alertas esperados.
- **Treinamento (geralmente):** Ensinar a sua equipe a usar a solução, interpretar os dados e responder aos incidentes.

11.3.2. **Para que serve?**

11.3.2.1. O serviço de instalação serve para garantir que você tenha a solução de monitoramento funcionando perfeitamente na sua rede. Sem ele, a solução seria apenas um software que não está entregando valor. É como comprar um carro e precisar de alguém para montá-lo e deixá-lo pronto para rodar.

11.3.2.2. Em resumo, ele transforma a "caixa" do software em uma ferramenta de segurança operacional e eficaz, protegendo sua rede contra ameaças complexas.

11.3.2.3. **É uma solução abrangente que combina:**

- **Hardware** para a **coleta e a interceptação** eficiente do tráfego de rede.
- **Software** para a **análise inteligente** desse tráfego, detecção de anomalias, identificação de ameaças e auxílio na resposta a incidentes.

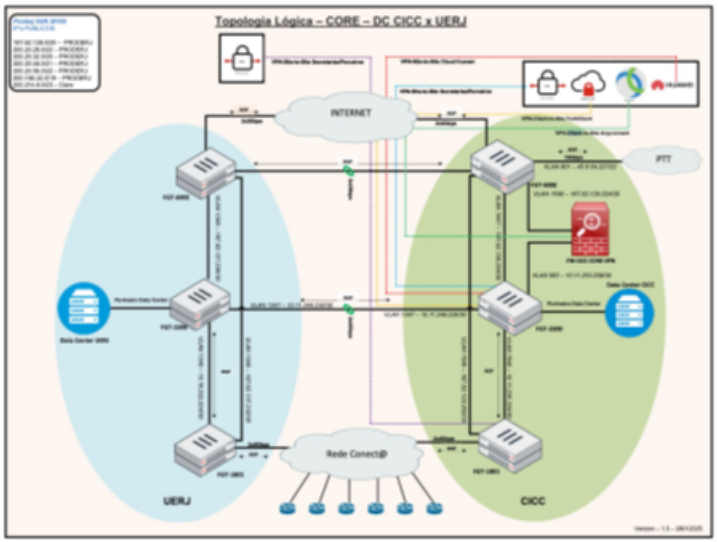
11.3.2.4. Ambos são essenciais para que a solução NDR funcione de forma eficaz, proporcionando visibilidade completa e inteligência sobre o que está acontecendo na rede para proteger contra ameaças sofisticadas.

11.3.2.5. Em resumo, essa solução serve para identificar ameaças de segurança que as ferramentas tradicionais podem não pegar, proteger sua rede contra ataques sofisticados e ajudar sua equipe a agir rapidamente para minimizar os danos de um incidente. É uma camada de defesa essencial em um cenário de cibersegurança em constante evolução.

11.4. **Memória de cálculo - item 1**

11.4.1. Dimensionar a compra de um equipamento NDR (Network Detection and Response) envolve a consideração de vários fatores para garantir que o sistema seja capaz de atender às necessidades de segurança da rede. O principal deles é o “volume de dados”. Conforme se observa da topologia descrita na figura abaixo, a rede a ser protegida (entrada de internet) tem um throughput de **2 Gbps,** pelo que entendemos como o mínimo necessário.

11.4.2. **Throughput de 2 Gbps** significa que a capacidade máxima de transferência de dados em uma rede ou conexão é de 2 gigabits por segundo, desta forma foi dimensionado o mínimo necessário de transferência de dados para utilização na rede do PRODERJ totalizando a **quantidade de 2.**



11.5. **Item 2 do Lote I- Serviço técnico especializado de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.**

11.5.1. Os **Serviços Técnicos Especializados** Serão utilizados na operacionalização da solução, com apoio presencial de pessoal especializado ou remoto caso definido pela contratante, devendo ser solicitado mediante emissão de ordem de serviço, informando as aplicações que farão parte do escopo do serviço.

11.5.2. Todas as atividades desempenhadas relativas aos **Serviços Técnicos Especializados** deverão ser executadas nas dependências da contratante ou de maneira remota caso definido pela contratante, respeitando o horário de funcionamento da mesma, e com o acompanhamento e ciência dos servidores.

11.5.3. Demais detalhamento do serviços Técnicos Especializados estão definidas no ANEXO II do Catálogo de Serviço.

11.5.4. **Memória de cálculo - item 2**

11.5.4.1. Trata-se do serviço técnico especializado tendo a quantidade de **6.080** serviço em UST, sob demanda.

11.5.4.2. **Memória de cálculo do catálogo de serviços para o item 2 do Lote I**

11.5.4.3. **Segue tabela abaixo a estimativa do quantitativo das subatividades relacionadas:**

Complexidade (Baixa, Média ou Alta)	Tipo de Execução (Remota ou Presencial)	Duração do Serviço (horas)	Validação dos Serviços Executados (horas)	Documentação dos Serviços Executados (horas)	Total Estimado de Horas	UST ajustada conforme a complexidade	Quantidade em 3 anos	Estimado de UST's
ATIVIDADES DE ARQUITETURA E PROJETO								
MÉDIA	PRESENCIAL	18	6	8	32	40	1	40
MÉDIA	PRESENCIAL	24	3	8	35	44	1	44
ALTA	PRESENCIAL	12	8	24	44	66	1	66
MÉDIA	PRESENCIAL	26	6	12	44	55	3	165
MÉDIA	PRESENCIAL	24	6	12	42	53	1	53
MÉDIA	REMOTO	6	1	2	9	11	1	11
ALTA	PRESENCIAL	15	4	8	27	41	2	81
MÉDIA	PRESENCIAL	18	6	10	34	43	3	128

ALTA	REMOTO	20	8	18	46	69	3	207
BAIXA	REMOTO	12	0	0	12	12	1	12
MÉDIA	PRESENCIAL	16	2	3	21	26	3	79
ALTA	PRESENCIAL	20	8	8	36	54	3	162
MÉDIA	PRESENCIAL	12	4	6	22	28	3	83
MÉDIA	REMOTO	8	1	2	11	14	3	41
MÉDIA	REMOTO	6	1	2	9	11	3	34
MÉDIA	REMOTO	6	1	2	9	11	3	34
ATIVIDADES DE MANUTENÇÃO CONTÍNUA								
MÉDIA	REMOTO	8	6	10	24	30	12	360
MÉDIA	REMOTO	8	1	2	11	14	6	83
MÉDIA	REMOTO	10	4	6	20	25	18	450
MÉDIA	REMOTO	8	2	4	14	18	6	105
MÉDIA	REMOTO	10	6	19	35	44	6	264
MÉDIA	REMOTO	12	4	5	21	26	6	156
MÉDIA	REMOTO	8	6	17	31	39	12	468
ALTA	PRESENCIAL	24	8	24	56	84	6	504
MÉDIA	REMOTO	24	0	0	24	30	2	60
MÉDIA	REMOTO	10	6	12	28	35	6	210
MÉDIA	REMOTO	8	6	12	26	33	6	198
ALTA	REMOTO	24	12	24	60	90	3	270
ALTA	REMOTO	24	12	24	60	90	6	540
ATIVIDADES ESPECIALIZADAS								
ALTA	PRESENCIAL	24	8	24	56	84	3	252
MÉDIA	PRESENCIAL	12	0	18	30	38	2	75
MÉDIA	REMOTO	12	6	10	28	35	3	105
MÉDIA	REMOTO	10	6	6	22	28	3	83
ALTA	REMOTO	16	2	3	21	32	6	192
MÉDIA	REMOTO	12	6	10	28	35	3	105
ALTA	REMOTO	70	0	10	80	120	3	360
TOTAL								**6.080**

11.6. **Item 3 do Lote I - Treinamento da Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.**

11.6.1. O treinamento da solução de monitoramento de comportamento anômalo é o serviço que ensina sua equipe a, de fato, usar e tirar o máximo proveito da ferramenta que foi instalada.

11.6.2. **O que o serviço faz:**

11.6.2.1. Este serviço foca em capacitar as pessoas que irão operar e gerenciar a solução no dia a dia. Isso geralmente inclui:

- **Entendimento da Solução:** Explicar como a solução funciona, quais são seus principais recursos e o que ela é capaz de fazer.
- **Operação:** Ensinar a navegar pela interface da ferramenta, gerar relatórios, configurar alertas e personalizar o monitoramento.

- **Análise de Incidentes:** Capacitar a equipe a interpretar os alertas de anomalias, entender o que eles significam, e identificar a gravidade e o impacto de um possível incidente de segurança.
- **Resposta a Incidentes:** Treinar a equipe sobre os passos a serem seguidos quando um incidente é detectado, como isolar sistemas, coletar evidências e mitigar os danos.
- **Boas Práticas:** Compartilhar as melhores práticas para manter a solução ajustada e eficaz ao longo do tempo.

11.6.3. **Para que serve:**

11.6.3.1. O treinamento serve para transformar a tecnologia em inteligência e ação. Sem ele, mesmo com a melhor solução instalada, sua equipe pode não saber como:

- **Identificar ameaças reais:** Diferenciar um alerta falso de um ataque verdadeiro.
- **Agir rapidamente:** Responder a um incidente de forma eficiente para minimizar os danos.
- **Otimizar a ferramenta:** Ajustar a solução para que ela se adapte melhor às necessidades específicas da sua rede.
- **Maximizar o investimento:** Garantir que o valor pago pela solução e sua instalação seja totalmente aproveitado.

11.6.3.2. Em resumo, o treinamento é crucial para que sua equipe esteja preparada e capacitada para proteger sua rede, utilizando a solução de monitoramento de forma eficaz e respondendo adequadamente a qualquer comportamento anômalo. É o que garante que a ferramenta não seja apenas um software, mas uma capacidade de defesa ativa em suas mãos.

11.7. **Memória de cálculo - item 3**

11.7.1. Para o Treinamento PRODERJ, o quantitativo de alunos será de 06 (seis), para a realização da capacitação.

11.8. **Item 4 do Lote II - Equipamento interceptador de tráfego**

11.8.1. O **equipamento para interceptação de tráfego** é uma peça central nas estratégias de segurança cibernética modernas, especialmente sob o conceito de Zero Trust (Confiança Zero), que parte do princípio de que você não pode proteger o que não consegue ver. Sua principal função é solucionar a falta de visibilidade na rede, um desafio crescente com o uso de criptografia de dados (TLS 1.3), virtualização e contêineres.

11.8.2. **O que é:**

11.8.2.1. Esse equipamento é um dispositivo de rede especializado que atua como um "filtro" inteligente. Ele é projetado para lidar com o fluxo de dados da rede e eliminar o processamento de informações irrelevantes para as plataformas de segurança, direcionando apenas o que é "inteligível" ou relevante para análise.

11.8.2.2. Ele opera em duas modalidades principais:

1) **In-line Bypass (em linha):** O equipamento se posiciona diretamente no caminho do tráfego do datacenter. Ele pré-processa os dados, e se alguma informação for relevante para a segurança, a roteia para as ferramentas de verificação. Caso contrário, o tráfego segue seu fluxo normal sem interrupções.
2) **Out-of-band (Espelhamento):** Nesta modalidade, o equipamento se conecta à rede física e cria uma cópia (espelho) do tráfego lógico, enviando-a para as ferramentas de segurança. Isso permite que as análises de segurança ocorram de forma passiva, sem interferir ativamente no fluxo de dados original da rede.

11.8.2.3. Para garantir a fluidez da comunicação mesmo em caso de falha, a solução prevê o uso de um componente passivo que não depende de energia elétrica. Isso é crucial porque, se o interceptador de tráfego (que está em linha na rede) sofrer um problema, a comunicação da rede não será interrompida, evitando uma falha generalizada no PRODERJ.

11.8.2.4. O equipamento, e sua arquitetura, também é escalável, permitindo a expansão da capacidade de processamento de tráfego conforme a demanda, com a adição de placas complementares, ou de novos equipamentos, para lidar com volumes crescentes de dados e funcionalidades de segurança.

11.8.3. **Para que serve:**

11.8.3.1. O equipamento de interceptação de tráfego serve para:

- **Prover Visibilidade Completa:** Garante que 100% do tráfego, tanto Leste-Oeste (comunicações internas entre servidores virtualizados e contêineres, muitas vezes invisíveis para ferramentas tradicionais) quanto **Norte-Sul** (tráfego de entrada e saída da rede), seja inspecionado e analisado.
- **Otimizar o Fluxo de Dados para Ferramentas de Segurança:** Atua como uma camada central de encaminhamento, filtrando e direcionando apenas o tráfego relevante para as diversas ferramentas de segurança (firewalls, IPS, anti-malware, etc.), evitando que elas processem dados desnecessários.
- **Melhorar a Eficiência Operacional:** Ao otimizar a análise de segurança, reduz o tempo gasto na validação do tráfego, o que é crítico para evitar impactos na infraestrutura de Tecnologia da Informação e Comunicação (TIC) do PRODERJ.
- **Suportar o Conceito de Zero Trust:** Ao garantir visibilidade total, habilita a implementação da premissa de que nenhuma entidade é confiável por padrão, permitindo a detecção de ameaças mesmo dentro da rede.

- **Garantir Alta Disponibilidade e Resiliência:** Com a previsão de duas unidades e módulos de bypass passivos (não energizados), assegura que a comunicação de rede não será interrompida em caso de falhas no equipamento de interceptação.
- **Permitir Escalabilidade:** Sua modularidade e a capacidade de expansão de processamento sob demanda permitem que a solução se adapte ao crescimento do volume de tráfego e à introdução de novas tecnologias de segurança.

11.8.3.2. Em suma, o equipamento de interceptação de tráfego é a base para uma segurança de rede eficaz e otimizada, fundamental para o PRODERJ garantir a proteção de sua infraestrutura e dados em um cenário de ameaças cada vez mais complexas e tráfego crescente.

11.8.4. **Item 4 do Lote II - Memória de cálculo**

11.8.5. Equipamento Interceptador de Tráfego e Módulo para Captura do Tráfego Inline e Componentes de Expansão Internos

11.8.6. Dentro do arquétipo desse tipo de solução, os equipamentos interceptadores de tráfego são responsáveis por filtrar todo o fluxo de pacotes e quadros de rede com o intuito de eliminar o processamento do conjunto de dados que não são inteligíveis por plataformas de segurança.

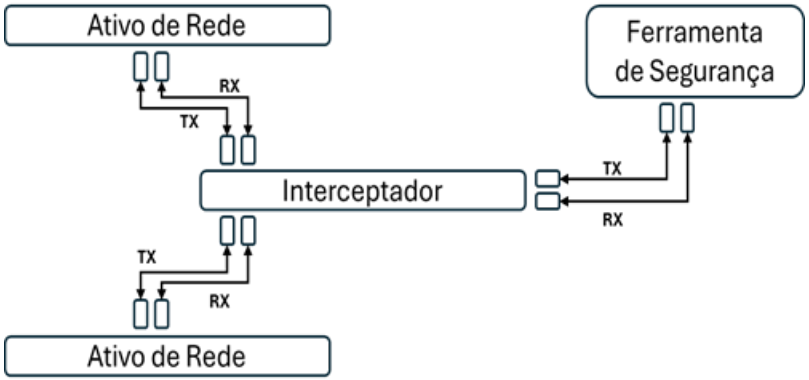
11.8.7. Esse tipo de solução emprega 2 (duas) modalidades operacionais, sendo elas:

a) In-line Bypass (em linha): Nessa modalidade, o equipamento atua como um elemento intermediário no tráfego lógico de Datacenter, de modo que internamente ao equipamento, os dados são pré-processados e caso sejam específicos dos contextos de análise de segurança, as informações são roteadas para as plataformas de verificação. Caso contrário, o tráfego flui no sentido tradicional, sem sofrer qualquer alteração.

b) Out-of-band (Espelhamento): Nessa modalidade, o equipamento é interconectado a rede física e o tráfego lógico é copiado, ou espelhado, para as ferramentas de segurança. Desse modo, as análises e rotinas operacionais das plataformas de segurança não requerem uma interceptação ativa do tráfego de dados, apenas uma resposta reativa.

c) Ademais, demonstramos em um diagrama como se espera que a solução se comporte dentro de nossa infraestrutura.

d) Na arquitetura do tráfego a seguir, observe que para os ativos da topologia existente, não há disponibilização na rede (nos cabeçalhos de controle das sessões), qualquer indicativo sobre a existência da ferramenta de filtragem dos dados, o processo é transparente para os sistemas digitais.



11.8.8. Entretanto, para que a solução funcione adequadamente, faz-se necessário dispor de um componente passivo, o qual executa as operações de cópia do tráfego e que não esteja energizado eletricamente.

11.8.9. Tal conceito se justifica dentro dos cenários nos quais uma falha possa ocorrer. Como o interceptador de tráfego se encontra entre os ativos de rede, caso um sinistro ocorra em sua própria operação, uma falha generalizada de rede poderia impactar o PRODERJ.

11.8.10. Desse modo, uma vez que a camada física fica vinculada a módulos que não dependem de energia elétrica, as comunicações não cessam diante de um problema que envolva o domínio de processamento da solução em si.

11.8.11. Sendo assim, para esta etapa de projeto, contempla-se 2 (duas) unidades de interceptadores, com o propósito de provermos alta disponibilidade entre eles e, por conseguinte, cada unidade possuirá 1 (um) módulo complementar para permitir a fluidez do tráfego em caso de falha elétrica ou de outro sinistro específico da solução.

11.8.12. Para cada equipamento, ponderou-se inicialmente o consumo de, ao menos 8 (oito) interfaces padrão 25/10 Gbps SFP – elas são retrocompatíveis; e, concomitantemente 4 (quatro) interfaces padrão 100 QSFP. Apesar das interfaces QSFP serem, também, retrocompatíveis com 40G, esse tipo de interconexão física não será utilizado em nosso ambiente.

11.8.13. Não obstante, esclarecemos que esse tipo de solução, também, permite através da sua modularidade a expansão da capacidade de processamento de tráfego, sob demanda. Nesse sentido, registraremos para cada equipamento 1 (uma) placa complementar por equipamento, a qual poderá incorporar uma quantidade ainda maior de tráfego de segurança do PRODERJ. Alternativamente, serão admitidas soluções com

escalabilidade horizontal para os casos de impossibilidade de fornecimento de soluções modulares.

11.8.14. Uma vez que existem distintas funcionalidades para a otimização do tráfego de segurança a ser filtrado, torna-se necessário prever a ampliação do poder de processamento da solução em função do consumo de recursos computacionais advindos das tecnologias a serem implementadas.

11.8.15. Através do rito formal de consumo fracionado de soluções de Tecnologia, alicerçado pelas regras e condições da Lei Federal 14.133/2021, o PRODERJ consegue através da segmentação dos itens que podem ser adquiridos futuramente, projetar os distintos cenários que necessitarão de expansão da solução tecnológica e, por conseguinte, executar o recurso financeiro diante da necessidade eminente que surgir durante a vigência contratual.

11.8.16. Esta é a métrica mais crítica para um equipamento de interceptação. Ele precisa ser capaz de lidar com o volume máximo de dados que passa pela rede, desta forma foi dimensionado o mínimo necessário de transferência de dados para utilização na rede do PRODERJ totalizando a **quantidade de 2.**

11.9. **Item 5 do Lote II - Licenciamento de desduplicação do tráfego.**

11.9.1. **Desduplicação**

11.9.1.1. Consiste na técnica de eliminação de payloads redundantes do tráfego a ser transmitido. Com o intuito de eliminar o consumo de recursos de processamento para o tratamento de tráfego de segurança, o uso da tecnologia permite a eliminação e a desoneração no tratamento de informações duplicadas.

Ressaltamos que esse tipo de tecnologia não deve eliminar conteúdo do tráfego e, apenas, referenciar dados para que não ocorra a sua retransmissão ou o processamento desnecessário.

11.9.2. **Item 5 do Lote II - Memória de Cálculo**

11.9.2.1. A desduplicação trabalha identificando blocos de dados repetidos. Para isso, ela gera um hash (uma espécie de "impressão digital" única e compacta) para cada bloco de dados que passa. Para identificar redundância, esses hashes precisam ser armazenados em memória (ou em estruturas de dados otimizadas) para comparação com os hashes de blocos recém-chegados. Um throughput alto significa uma taxa elevada de geração e comparação de hashes, demandando mais memória para o cache desses hashes e suas referências, desta forma foi dimensionado o **mínimo necessário de 2 (duas) unidades,** uma por equipamento físico presente.

11.9.3. **Item 6 do Lote II - Licenciamento avançado de descriptação do tráfego.**

11.9.4. **Descriptação**

11.9.4.1. A tecnologia de descriptografia, ou abertura do tráfego, permite que a solução possa analisar, também, as sessões de aplicações que se comunicam através de payloads cifrados, como aquelas que se comunicam (TLS e similares).

11.9.4.2. Uma vez que esse tipo de técnica é intrinsicamente necessária para a validação do tráfego, principalmente se remetido a usuários finais (rotineiramente trafegando em plataformas Web TLS), e aplicações Web, torna-se essencial deter desse mecanismo para abertura e filtragem do tráfego.

11.9.4.3. Ressaltamos que esse tipo de tecnologia, além de demandar sua existência para o contexto de segurança da informação, também é essencial a depender do tipo de topologia implementada (vide tópico sobre modalidades de implantação).

11.9.4.4. Uma vez que algumas ferramentas exigem a recepção de tráfego não cifrado (descriptografado), para poderem analisar o conteúdo de segurança ou de observação, torna-se notório que detenhamos da tecnologia a nosso dispor dentro do PRODERJ.

11.9.5. **Item 6 do Lote II - Memória de Cálculo**

11.9.5.1. A solução precisa ter memória suficiente para "bufferizar" os dados enquanto eles são descriptografados, inspecionados, e depois re-criptografados antes de serem enviados ao destino. Isso é especialmente relevante para evitar gargalos de desempenho. Em resumo, a memória é vital para que a solução consiga "abrir" o tráfego criptografado em tempo real, mantendo a performance da rede e permitindo que as ferramentas de segurança (como o monitoramento de comportamento anômalo) tenham visibilidade total sobre o conteúdo que, de outra forma, estaria "oculto". desta forma foi dimensionado o mínimo necessário de 2 (duas) unidades, uma por equipamento físico presente.

11.9.6. **Item 7 do Lote II - Licenciamento avançado de análise de aplicações**

11.9.7. **Análise de Aplicações**

11.9.7.1. **Item 7 do Lote II - Licenciamento avançado de análise de aplicações:** Para a análise de aplicações, duas classificações dos payloads do tráfego são essenciais, sendo elas a própria análise do conteúdo das aplicações ou o conjunto de metadados (“dados sobre dados”), que representam elas.

11.9.7.2. A habilidade da solução em classificar aplicações nos permite determinar os melhores cenários em que uma tomada de decisão específica se remete para as ferramentas de segurança que precisarão analisar o contexto de uso daquele tráfego.

11.9.7.3. O intuito desse tipo de tecnologia é de prover informações de alto nível, que envolvem ações não autorizadas por aplicações, comportamentos anômalos de usuários e, principalmente, a garantia da experiência do usuário.

11.9.7.4. Para promovermos uma melhor observabilidade do tráfego, determinamos esse contexto, também, como uma possível tecnologia a ser consumida pelo PRODERJ dentro dessa contratação.

11.9.7.5. Por outro lado, quando falamos de contextos de observabilidade (por exemplo, a plataforma Elastic Search), a filtragem do tráfego para a análise somente das informações sobre o tráfego, metadados, é suficiente para gerar resultados pelas plataformas que recebem os pacotes otimizados.

11.9.7.6. Uma vez que apenas o tráfego “limpo”, representado pelos metadados, é reencaminhado a plataforma de observação do tráfego, se reduz o consumo de NetFlows ou de um grande volume de informações completas de syslog a ser ingerido pelo receptor dos dados.

11.9.7.7. Por conseguinte, a determinação correta dos atributos que representam a informação buscada, dentro de um contexto de volume de tráfego, é suficiente para a análise final das ferramentas que enriquecem o detalhamento do consumo tecnológico do ambiente.

11.9.7.8. Nesse sentido, com o intuito de disponibilizar ainda mais capacidade de tomadas de decisões, pelo PRODERJ, o enriquecimento das informações e a otimização do consumo desse tráfego tem de ser contabilizado neste escopo de contratação.

11.9.8. **Item 7 do Lote II - Memória de Cálculo**

11.9.8.1. Em um ambiente com 2 equipamentos, a solução está analisando um fluxo constante e massivo de pacotes. A memória é usada para bufferizar esses pacotes temporariamente enquanto a classificação acontece, além de armazenar as estruturas de dados necessárias para a identificação da aplicação e a extração dos metadados. Um tráfego muito variado (com muitos tipos de aplicações diferentes) também exige mais memória para gerenciar a diversidade das classificações. Esclarece-se, por conseguinte, que neste escopo de contratação, foram registradas 2 (duas) unidades, uma por equipamento registrado, totalizando **a quantidade de 2.**

11.9.8.2. **Item 8 do Lote II - Licenciamento avançado de análise de metadados:** Além de analisar o conteúdo completo dos pacotes (o que pode ser intensivo), a NDR também gera e analisa metadados do tráfego (origem, destino, portas, protocolos, volumes, tempos de conexão). Este licenciamento permite uma análise profunda desses metadados para identificar padrões de comportamento, como varreduras de porta, comunicação com IPs maliciosos conhecidos, ou transferências de dados anormais, sem precisar inspecionar cada byte do conteúdo.

11.9.9. **Item 8 do Lote II - Memória de Cálculo**

11.9.10. A funcionalidade de análise de metadados representa um dos pilares da arquitetura de visibilidade inteligente. Trata-se de uma abordagem que ultrapassa o mero espelhamento ou encaminhamento bruto de pacotes, viabilizando a extração, tratamento e encaminhamento seletivo de informações contextuais (metadados) extraídas do tráfego de rede, com o objetivo de otimizar a atuação das ferramentas de segurança, observabilidade e monitoramento. Esclarece-se, por conseguinte, que neste escopo de contratação, foram registradas 2 (duas) unidades, uma por equipamento registrado, totalizando a **quantidade de 2.**

11.9.11. **Item 9 do Lote II - Módulo de expansão do processamento.**

11.9.12. Módulo de expansão do processamento: À medida que o volume de tráfego da rede cresce ou as ameaças se tornam mais complexas, a demanda por capacidade de processamento na solução de interceptação também aumenta. Este módulo permite adicionar mais poder de CPU e memória ao equipamento, ou sua ampliação em uma arquitetura horizontal, garantindo que ele possa lidar com grandes volumes de dados e realizar análises complexas em tempo real.

11.9.13. Fora contabilizado 1 (um) módulo de expansão por equipamento físico registrado, ou seja, 2 (duas) unidades.

11.9.14. Ele permite que a solução:

- **Lide com o aumento do tráfego**, processando mais dados sem gargalos.
- Realize **análises de ameaças mais complexas**, utilizando algoritmos avançados, machine learning e IA que exigem muitos recursos.
- Conduza **análises aprofundadas (DPI)** no conteúdo dos pacotes sem comprometer a performance.
- **Reduza falsos positivos/negativos** por meio de análises mais precisas.
- Mantenha a **resposta em tempo real** a incidentes.
- **Previna novas formas de ataque**, ao possibilitar a implementação de novas capacidades de detecção que demandam mais processamento.

11.9.15. A funcionalidade de análise de metadados representa um dos pilares da arquitetura de visibilidade inteligente. Trata-se de uma abordagem que ultrapassa o mero espelhamento ou encaminhamento bruto de pacotes, viabilizando a extração, tratamento e encaminhamento seletivo de informações contextuais (metadados) extraídas do tráfego de rede, com o objetivo de otimizar a atuação das ferramentas de segurança, observabilidade e monitoramento. Esclarece-se, por conseguinte, que neste escopo de contratação, foram registradas 2 (duas) unidades, uma por equipamento registrado, totalizando a **quantidade de 2.**

11.9.16. **Item 9 do Lote II - Memória de Cálculo**

11.9.17. A necessidade de expansão de processamento para sua solução NDR é justificada pela análise da sua performance atual, que revela se o volume de tráfego, a utilização dos recursos (CPU, RAM, I/O) e a eficácia da detecção estão no limite ou já comprometidos, especialmente ao considerar as funcionalidades avançadas (como DPI ou ML) ativadas, indicando que a "memória de cálculo" atual é insuficiente para as demandas presentes e futuras, desta forma foi dimensionado o mínimo necessário a **quantidade de 2.**

11.9.18. **Item 10 do Lote II - Módulo de Expansão para a Captura do Tráfego “Inline”**

11.9.18.1. **O que é:**

11.9.18.2. Um Módulo de Expansão para a Captura do Tráfego "Inline" é um componente de hardware adicional que pode ser integrado a um equipamento de interceptação do tráfego.

11.9.18.3. Ele permite que o equipamento, que normalmente funcionaria de forma passiva (apenas copiando o tráfego para análise), passe a operar diretamente no fluxo de dados da rede. Ou seja, em vez de apenas "ouvir" o tráfego, ele se posiciona em linha no caminho da comunicação.

11.9.18.4. Essencialmente, este módulo adiciona a capacidade de o equipamento interceptar ativamente, inspecionar, e potencialmente manipular ou bloquear o tráfego em tempo real, antes que ele chegue ao seu destino final ou a outras partes da rede.

11.9.18.5. Em resumo, enquanto a função principal de uma solução de interceptação do tráfego é de filtrar o tráfego para o correto processamento pelas soluções de segurança, o Módulo de Expansão para a Captura do Tráfego "Inline" eleva a capacidade da solução, adicionando o poder de intervir ativamente e prevenir situações em tempo real.

11.9.18.6. **Item 10 do Lote II - Memória de Cálculo**

11.9.18.7. Se faz necessária para um módulo NDR de captura de tráfego "inline", é crucial considerar: o volume atual e projetado do tráfego de rede (Gbps/Mbps) a ser inspecionado, a complexidade das regras de segurança a serem aplicadas, a profundidade da inspeção (DPI) exigida, e o desempenho atual do seu equipamento NDR, para evitar gargalos e garantir que ele suporte futuras ameaças e crescimentos, desta forma foi dimensionado o mínimo necessário a **quantidade de 2.**

11.9.18.8. **Item 11 do Lote II - Licenciamento para o gerenciamento centralizado da solução**

11.9.19. Em implementações maiores, com múltiplos equipamentos espalhados por diferentes locais ou data centers, é essencial ter uma **plataforma centralizada** para configurar, monitorar e gerenciar todos esses componentes. Este licenciamento habilita essa console unificada, que facilita a operação, a visualização de alertas e a resposta a incidentes.

11.9.20. **Item 11 do Lote II - Memória de Cálculo**

11.9.21. **Gerenciamento Centralizado das Soluções**

11.9.21.1. Ademais, esclarecemos que a contratação é composta por:

a) 2 (dois) equipamentos de interceptação do tráfego;

b) 1 (um) interceptador virtualizado;

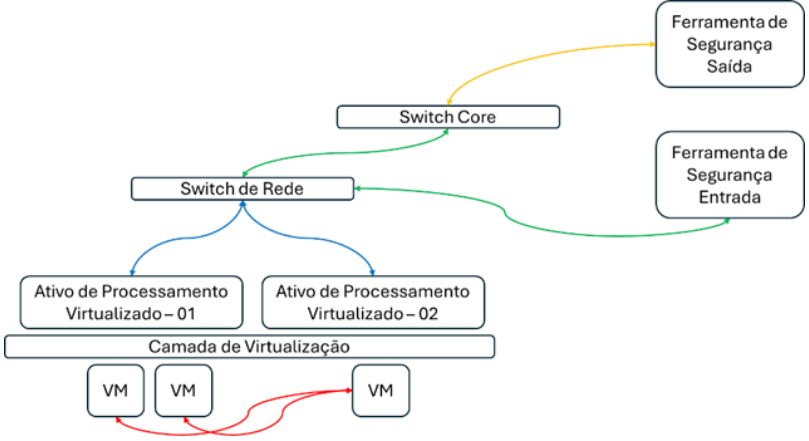
c) 1 (um) concentrador do tráfeo.

11.9.21.2. Portanto, para podermos gerenciar todos os elementos, de modo unificado, contabilizamos uma plataforma de gestão centralizada que deverá contabilizar, concomitantemente, a gestão de todos os elementos a serem contratados. Nesse escopo, admitiremos plataformas de gerenciamento físicas ou virtualizadas, desde que capazes de prover administração centralizada e facilitada ao PRODERJ. Trata-se do licenciamento para gerenciar a solução totalizando a **quantidade de 1 licença.**

11.9.21.3. **Item 12 do Lote II - Interceptador do tráfego virtualizado avançado.**

11.9.22. **Interceptador do tráfego virtualizado avançado:** Em ambientes de nuvem ou data centers virtualizados, o tráfego não flui por cabos físicos tradicionais, mas sim por redes virtuais. Este software ou componente permite que a solução interceptação "enxergue" e intercepte o tráfego que ocorre entre máquinas virtuais (VMs), contêineres e outras cargas de trabalho virtuais, garantindo visibilidade completa em ambientes modernos e dinâmicos.

11.9.22.1. Sendo assim, apenas 1 (uma) unidade será registrada para que possamos integrar nosso ambiente operacional.



11.9.23. **Item 12 do Lote II - Memória de Cálculo**

11.9.24. Diante do cenário previsto nesta contratação, cabe esclarecer as diferentes topologias de rede que devem ser interceptadas pela solução:

a) Quando se emprega, na topologia, plataformas de segurança da informação que se aproximam da saída de rede (Firewalls, IPS, IDS, Proxy, etc.), o tráfego físico (representado pelas cores amarela e verde na imagem acima), deve ser tratado por equipamentos físicos (vide o equipamento de interceptação de tráfego da contratação), pois do ponto de vista de fluxo de dados, essa é a rota mais otimizada e que evita "loops" de rede (ida e retorno do tráfego a ser processado e filtrado).

b) Por outro lado, quando observamos o tráfego virtualizado, referente as comunicações entre máquinas virtuais – plataformas de segurança; não se justifica desviar o tráfego (sair das rotas vermelhas e azuis para adentrar nas verdes ou amarelas, da imagem anterior), para que ele seja processado, filtrado e retornado ao ambiente de virtualização.

c) Desse modo, para que possamos garantir a interceptação do tráfego como um todo dentro do nosso ambiente de comunicação, computaremos uma unidade de interceptação virtual, a qual deterá de todas as habilidades do equipamento em si, todavia, com sua designação específica para filtrar o tráfego do ambiente virtualizado do PRODERJ.

d) **Sendo assim, apenas 1 (uma) unidade será registrada** para que possamos integrar nosso ambiente operacional.

11.9.25. **Item 13 do Lote II - Chassi para interconector passivo de interceptação do tráfego - interfaces ópticas**

11.9.25.1. Um **chassi** é uma estrutura que abriga outros módulos. Neste caso, ele serve para interligar passivamente (sem interferir no tráfego) as interfaces ópticas que coletarão o tráfego de redes de fibra óptica. É a base para a conexão.

11.9.25.2. A principal finalidade desse chassi é **fornecer visibilidade abrangente e segura sobre o tráfego de redes de fibra óptica**, que é essencial para segurança e monitoramento. Ele serve para:

1) **Coleta Segura e Não Intrusiva de Tráfego:** Permite que você "espelhe" ou colete uma cópia exata do tráfego de fibra óptica sem precisar cortar a rede ou inserir dispositivos ativos que possam falhar e interromper a comunicação. É ideal para missões críticas onde a interrupção não é uma opção.
2) **Alimentar Ferramentas de Segurança e Monitoramento:** Fornece a entrada de dados para soluções como:

- **NDR (Network Detection and Response):** Para detecção de ameaças, comportamento anômalo e resposta a incidentes.
- **SIEM (Security Information and Event Management):** Para correlação de eventos de segurança.
- **Analisadores de Pacotes:** Para análise forense detalhada.
- **Ferramentas de Desempenho de Rede (NPMD):** Para otimização e solução de problemas.

11.9.25.3. Fora computado 4 (quatro) chassis para embarcar múltiplos interconectores passivos e atender a arquitetura do PRODERJ.

11.9.25.4. **Item 14, Item 15 e Item 16 do Lote II - Chassi e Interconectores Passivos De Interceptação do Tráfego – RJ-45/SFP/QSFP**

11.9.25.5. Conforme elencado anteriormente, dentro da topologia física de interconexão dos enlaces de comunicação do PRODERJ, uma opção a ser viabilizada tange o escopo de implantação de uma solução que copia os dados a serem filtrados sem a necessidade da interceptação ativa do tráfego – modalidade out-of-band.

11.9.25.6. Um dos grandes benefícios da solução é a possibilidade de combinar seu uso com os interconectores passivos, que são módulos que permitem a cópia completa do tráfego, do ambiente do PRODERJ, sem afetar o fluxo dos dados.

11.9.25.7. São tomados como componentes passivos, a serem dispostos na arquitetura do PRODERJ, sem a injeção de sinal no meio.

11.9.25.8. Por serem independentes dos demais equipamentos de rede, como switches e roteadores, eles permitem que as ferramentas de segurança recebam os dados capturados em diferentes pontos da infraestrutura, sem interferir com o funcionamento da rede.

11.9.25.9. Embora existam recursos nativos nos switches para espelhamento de portas (SPAN), habilitar essa funcionalidade neles pode causar alguns problemas, incluindo descarte de pacotes de links muito utilizados, filtragem de erros de camada física, sobrecarga do processamento do switch e congestionamento de tráfego, levando a problemas de desempenho e aumento nos tempos de resposta, além de vulnerabilidades a ataques.

11.9.25.10. O uso dos interconectores passivos alivia esse impacto, pois, além de não onerar o processamento dos equipamentos de rede para habilitar a visibilidade do tráfego, eles suportam a construção de uma arquitetura agnóstica de rede, com visibilidade completa e detalhada do tráfego, permitindo o monitoramento, e análise de desempenho da rede de maneira eficiente.

11.9.25.11. Cabe ressaltar que, na arquitetura, os interconectores passivos apoiam na flexibilidade de implantação da cópia do fluxo de dados.

11.9.25.12. Uma vez que pode se tornar complexa a manobra de movimentação e migração dos enlaces físicos, ainda mais se considerando que os equipamentos principais não necessariamente estarão fisicamente no mesmo rack que os demais ativos de rede, os componentes aqui definidos viabilizam a construção técnica da solução através de um viés de mitigação da alteração das nossas próprias comunicações.

11.9.25.13. **Item 14, Item 15 e Item 16 do Lote II - Memória de Cálculo**

11.9.25.14. Face ao exposto, destacamos que inicialmente, contabilizou-se **4 (quatro) unidades para cada item** de Chassi, interconector passivo, por tipo de interconexão física, a ser registrado no processo para consumo futuro do PRODERJ – RJ-45, SFP e QSFP.

11.9.25.15. Uma vez que os componentes dependem de um invólucro para serem acomodados corretamente nas nossas instalações físicas, ele também fora determinado no processo com a mesma quantidade.

11.9.26. **Item 17 do Lote II - Concentradores De Tráfego**

11.9.26.1. Dentro da arquitetura de interceptação de tráfego, existe uma limitação natural do ambiente que se relaciona com o volume de interfaces físicas disponíveis para acomodar o tráfego a ser filtrado.

11.9.26.2. Os equipamentos concentradores de tráfego costumam ampliar essa densidade, permitindo a escalabilidade das interconexões físicas através da concentração de múltiplos segmentos de rede na solução.

11.9.26.3. Tendo em vista a natureza do PRODERJ em prestar serviços, não só de Tecnologia da Informação, mas também, de Comunicações e Rede, a necessidade do equipamento surge com cunho específico de acomodar essa possível expansão.

11.9.26.4. Uma vez que todo o contexto da contratação se categoriza como um investimento sob demanda, ou seja, com seu desprendimento financeiro somente em real função da demanda técnica, registraremos **1 (uma) unidade,** composta por 48 (quarenta e oito) padrão SFP e 8 (oito) interfaces padrão QSFP.

11.9.26.5. Ressaltamos, ainda, que esse tipo de solução não se comporta como um switch, pois funções básicas de filtragem de tráfego são executadas pelo equipamento e não apenas a alteração dos cabeçalhos de pacotes das sessões de transporte.

11.9.27. **Item 18, Item 19, Item 20 e Item 21 do Lote II - Transceivers**

11.9.27.1. Inicialmente, o PRODERJ considerou que para atendemos a demanda inicial, 4 (quatro) transceivers de 25Gbps seriam necessários para operacionalizarmos cada interceptador de tráfego.

11.9.27.2. No entanto, contabilizamos transceivers adicionais, não só para permitir a expansão das interconexões, mas também para podermos contornar situações técnicas em que possa existir a falta de compatibilidade física da solução com a rede do PRODERJ. Totalizando a quantidade de **8 por equipamento.**

11.9.27.3. Desse modo, se esclarece:

Componente	Transceivers Inclusos por Equipamento	Total de Portas	Quantidade que pode requerer transceivers	Qtd. para 2 equipamentos
1G RJ/45	0	0	4	8
10G SFP28	4	8	4	8
25G SFP28	4	8	4	8
100/40G QSFP28	0	4	4	8

11.9.27.4. O intuito com a quantidade determinada é garantir que não somente o escopo pretendido possa ser maximizado, mas também, possamos contornar demais interconexões do ambiente em caso de necessidade.

11.9.27.5. Não obstante, destacamos que os transceivers, alternativamente, também poderão ser empregados no equipamento concentrador de tráfego previsto com a solução, garantindo maior flexibilidade ao PRODERJ.

11.9.28. **Item 22 do Lote II - Do Quantitativo de Serviços e Memória de cálculo - UST**

11.9.28.1. Como métrica universal para o consumo de múltiplos serviços correlatos a contratação, os quais contemplam a implantação, a manutenção evolutiva, a manutenção corretiva, a segurança da informação e o treinamento operacional da solução, se determinou a seguir o montante de Unidades de Serviço Técnico dimensionadas em conformidade com a necessidade do PRODERJ.

11.9.28.2. Na memória de cálculo o dimensionamento ponderado levou em consideração a possibilidade de execução de todo o montante de recursos previstos para consumo durante a vigência contratual.

11.9.28.3. Essa quantidade foi empregada como métrica de quantidade na tabela a seguir, exceto nos quantitativos diferentes apresentados, os quais indicam métricas empíricas nossas para consumo ao longo do período contratual.

11.9.28.4. O quantitativo e distribuição das UST previstas, considerou as seguintes características:

a) O Catálogo de serviço será executado por profissionais técnicos e especialistas e que cada tarefa exige um ou mais perfis profissionais;

b) Para os quantitativos estimados por cada atividade, considerou o tipo de profissional que executará um ou mais desenvolvimentos ao mesmo tempo na atividade;

c) Os quantitativos estimados mensais, bem como o detalhamento das atividades e suas descrições previstas em catálogo poderão ser ajustadas em razão da qualificação e da quantidade de demandas efetuadas, e em função dos redirecionamentos da projeção estratégica da Instituição Governamental ou do plano diretor da área;

d) Alterações, inclusões e exclusões são previsíveis visto que a implementação do tipo de demanda, depois de concluída, gerará um grupo de novos procedimentos e novas atividades rotineiras a serem executadas com o objetivo de manter a disponibilidade e a continuidade do novo processo implantado; e

e) As estimativas utilizadas basearam-se em pesquisas de mercado que demonstram em média **3.238 (três mil duzentos e trinta e oito)USTs.** para Serviços Técnicos Especializados (sob demanda) durante uma vigência contratual de uma única Unidade Gestora, conforme ANEXO IV - CATÁLOGO DE SERVIÇOS, deste documento.

11.9.28.5. **Memória de cálculo do catálogo de serviços para o Lote II.**

11.9.28.6. **Segue tabela abaixo a estimativa do quantitativo das subatividades relacionadas:**

Complexidade (Baixa, Média ou Alta)	Tipo de Execução (Remoto ou Presencial)	Duração do Serviço (horas)	Validação dos Seviços Executados (horas)	Documentação dos Serviços Executado (Horas)	Total Estimado de Horas	UST AJUSTADA CONFORME A COMPLEXIDADE	Quantidade em 3 anos	ESTIMADO DE USTs
ATIVIDADES DE ARQUITETURA E PROJETO								
MEDIA	PRESENCIAL	24	4	24	52	65	2	130
ALTA	PRESENCIAL	36	6	12	54	81	2	108
MEDIA	REMOTO	12	6	8	26	32	2	52
MEDIA	REMOTO	16	6	8	30	37	2	60
MEDIA	PRESENCIAL	12	2	8	22	27	2	44
ALTA	PRESENCIAL	6	6	3	15	22	2	30
ALTA	PRESENCIAL	8	1	8	17	25	2	34
ALTA	PRESENCIAL	5	1	3	9	13	2	18
MEDIA	REMOTO	6	1	3	10	12	2	20
ALTA	REMOTO	6	1	3	10	15	2	20
ALTA	REMOTO	6	1	3	10	15	2	20
MEDIA	REMOTO	6	1	3	10	12	2	20
ALTA	REMOTO	6	1	3	10	15	2	20
MEDIA	REMOTO	4	1	3	8	10	2	16

MEDIA	REMOTO	4	1	3	8	10	2	16
MEDIA	REMOTO	4	1	3	8	10	2	16
ALTA	REMOTO	8	1	3	12	18	2	24
ALTA	PRESENCIAL	4	1	3	8	12	2	16
MEDIA	REMOTO	4	1	3	8	10	2	16
ALTA	REMOTO	48	1	3	52	78	2	104
MEDIA	REMOTO	6	1	3	10	12	2	20
ALTA	PRESENCIAL	8	1	3	12	18	2	24
MEDIA	REMOTO	12	1	3	16	20	2	32
BAIXA	REMOTO	48	0	0	48	48	2	96
ATIVIDADES DE MANUTENÇÃO CONTÍNUA								
BAIXA	REMOTO	4	1	3	8	8	2	16
BAIXA	REMOTO	4	1	3	8	8	2	16
MEDIA	REMOTO	6	1	3	10	12	2	20
MEDIA	REMOTO	4	1	3	8	10	2	16
MEDIA	REMOTO	4	1	3	8	10	2	16
ALTA	REMOTO	4	1	3	8	12	2	16
ALTA	REMOTO	2	1	3	6	9	2	12
MEDIA	REMOTO	2	1	3	6	7	2	12
MEDIA	REMOTO	3	1	3	7	8	2	14
MEDIA	REMOTO	4	1	3	8	10	2	16
MEDIA	REMOTO	3	1	3	7	8	2	14
BAIXA	REMOTO	2	1	3	6	6	2	12
BAIXA	REMOTO	6	1	3	10	10	2	20
MEDIA	REMOTO	4	1	3	8	10	2	16
MEDIA	REMOTO	8	1	3	12	15	2	24
MEDIA	REMOTO	6	1	3	10	12	2	20
MEDIA	REMOTO	12	1	3	16	20	2	32
ALTA	REMOTO	24	1	3	28	42	2	56
MEDIA	REMOTO	6	1	3	10	12	2	20
MEDIA	REMOTO	16	0	0	16	20	2	32
MEDIA	REMOTO	4	1	3	8	10	2	16
MEDIA	REMOTO	4	1	3	8	10	2	16
MEDIA	REMOTO	3	1	3	7	8	2	14
MEDIA	REMOTO	4	1	3	8	10	2	16
ATIVIDADES ESPECIALIZADAS								
MEDIA	REMOTO	24	0	3	27	33	6	162
ALTA	REMOTO	30	0	3	33	49	2	66
ALTA	REMOTO	12	2	3	17	25	2	34
MEDIA	REMOTO	8	1	3	12	15	6	72

ALTA	REMOTO	24	1	3	28	42	2	56
ALTA	REMOTO	36	1	3	40	60	2	80
MEDIA	REMOTO	30	1	3	34	42	6	204
ALTA	REMOTO	30	1	3	34	51	2	68
ALTA	REMOTO	48	0	0	48	72	2	96
ALTA	REMOTO	40	2	3	45	67	2	90
ALTA	REMOTO	60	2	3	65	97	2	130
ALTA	REMOTO	36	2	3	41	61	2	82
MEDIA	REMOTO	12	0	0	12	15	36	432
ALTA	REMOTO	40	1	3	44	66	2	88
MEDIA	REMOTO	30	1	3	34	42	2	68
ALTA	REMOTO	12	2	3	17	25	2	34
MEDIA	REMOTO	24	2	3	29	36	2	58
TOTAL DE USTS								**3.238**

11.9.29. **Item 23 do Lote III - Licenciamento Elastic Enterprise On-Premises.**

11.9.29.1. Em uso, atualmente no PRODERJ, se encontra a versão gratuita da plataforma Elastic Search. A ferramenta em questão, além de atuar como um consolidador de eventos de segurança da informação para o apoio na tomada de decisões (SIEM), também é capaz de disponibilizar outras informações para a rotina operacional do PRODERJ, como:

a) Análise de conjuntos numéricos;

b) Análise de documentos de texto;

c) Classificação e ordenação de dados do PRODERJ.

11.9.29.2. Neste diapasão, é importante enfatizar que, os meios de interação do PRODERJ com os demais órgãos do estado ocorrem através de meios digitais e oportuniza a disponibilização de grandes massas de dados, as quais, estando disponíveis, permitem serem trabalhadas, apresentando o potencial de gerar informações e conhecimento.

11.9.29.3. Esta contratação é fundamentada na necessidade de uso de uma solução de busca e análise de dados baseado em índice invertido que possa lidar eficientemente com pesquisas textuais, numéricas e em dados não estruturados.

11.9.29.4. A agilidade na obtenção de informações é essencial para as atividades fins e meios desenvolvidos pelo PRODERJ, permitindo o acesso rápido a dados relevantes e a identificações de padrões e tendências.

11.9.29.5. Justifica-se ainda em do PRODERJ enfrentar desafios cada vez maiores no que diz respeito à busca e análise de dados em suas mais diversas áreas de atuação. Diante desse cenário, há a necessidade de uma contratação que seja capaz de atender a essa realidade crescente.

11.9.29.6. Deste modo, a fim de propiciar ao PRODERJ uma administração mais eficiente e ágil, há necessidade de utilização de uma solução de busca e análise de dados, comumente aplicados em análises de logs (envolve pesquisar, analisar e visualizar dados de máquinas gerados por sistemas de tecnologia da informação e infraestrutura de tecnologia), pesquisa de texto, inteligência de segurança, bem como, inteligência operacional, capazes de atender diferentes casos de usos, que permeiam as suas mais diversas áreas, contribuindo assim para o gerenciamento e a mineração constante de dados, com vistas a identificação de oportunidades e direcionamentos autômatos de ações predeterminadas.

11.9.29.7. Para uma melhor compreensão, como definição técnica bastante didática, podemos inferir que, solução de busca e análise de dados consiste em um conjunto de ferramentas que permite a coleta, armazenamento, pesquisa, análise e visualização de grandes volumes de dados, facilitando a obtenção de informações de negócio para a tomada de decisões estratégicas, resolução de problemas e o monitoramento de sistemas.

11.9.29.8. Por conseguinte, urge indispensável uma solução de busca e análise de dados baseado em índice invertido que possa encontrar e indexar dados de forma rápida, efetiva e escalável e que seja compatível e otimizado para a utilização em pesquisas textual, numérica, geoespaciais e em dados estruturados e não-estruturados.

11.9.29.9. A ferramenta tem uma complexidade técnica significativa, abrangendo aspectos essenciais como: indexação, consultas, escalabilidade, desempenho, e segurança, assim, a contratação de um serviço especializado é crucial para garantir uma implementação bem-sucedida e eficiente, permitindo que o PRODERJ, aproveite ao máximo as funcionalidades da solução.

11.9.29.10. Diante da necessidade exposta, denota-se no sentido de ser cognoscível que, a solução do Elastic Search Open Source utilizada hoje é limitada, ou seja, encontra-se incompleta para as exigências e os requisitos do parque tecnológico e da robusta infraestrutura de tecnologia da informação do PRODERJ.

11.9.30. **Item 23 do Lote III - Memória de Cálculo**

11.9.30.1. Para a formação do dimensionamento da solução, a seguinte memória de cálculo fora computada:

Tipo de Infraestrutura	Eventos por segundo (Médio)	QTD de Infraestrutura do PRODERJ	TOTAL DE EVENTOS
Endpoints (Notebooks / Desktops)	0,02	2946	58,92
Switches	150,00	60	9.000,00
Roteadores	5,00	10	50,00
Aplicações*	225,00	2000	450.000,00
Firewalls	1.500,00	8	12.000,00
VPNs (Enlaces Lógicos)	150,00	60	9.000,00
TOTAL			**480.109,00**

*Inclui servidores que hospedam múltiplas aplicações.

11.9.30.2. A quantidade de eventos por segundo e os seus pesos foram computados de acordo com guias de dimensionamento de múltiplas soluções gratuitas. Apesar de representarem uma média, tão somente, os quantitativos nos norteiam quanto ao volume de licenças e ao tamanho da infraestrutura para hospedar a solução.

11.9.30.3. Como taxa de conversão média, temos que 1 (um) evento corresponde a 100 Bytes de informações de controle, o que implica em um total de 0,048 GBytes por segundo, ou 4,05 GiB/dia, de informações capturadas pela plataforma.

11.9.30.4. Ao contabilizarmos a recomendação da fabricante quanto ao dimensionamento da solução atingimos o seguinte resultado:

Dimensionamento da Solução(https://www.elastic.co/blog/benchmarking-and-sizing-your-elasticsearch-cluster-for-logs-and-metrics)	
Primeira Etapa	
Volume de Dados (TiB) [a]	4,05
Dias de Retenção [b]	30
Réplicas [c]	0
Fator de Compressão [d]	2
Resultado [A]	A = a x b x (c + 1) x d243,06 TiB
Segunda Etapa	
Limiar de Marca d'água da Solução [e]	1 + 0,15 + 0, 1 (fator de erro)
Resultado [B]	A x e
Terceira Etapa	
Memória por Nó [f]	64
Proporção de Memória por Volume de Dados [g]	64 / 243,06
Resultado [C]	B / f / g(16,73)

11.9.30.5. Uma vez que a própria solução utiliza licenças de 64 GB, esse foi o montante contabilizado na linha [f], pois o PRODERJ espera consumir um servidor inteiro por licenças na solução.

11.9.30.6. Tendo em vista que a nossa necessidade inicial atinge o volume de 17 (dezessete) licenças, para comportar todo nosso ambiente, registaremos licenças adicionais, seja para a construção de réplicas do ambiente, em menor escala, ou até mesmo para permitir a escalabilidade da infraestrutura atual. Sendo assim, registraremos **24 (vinte e quatro) licenças.**

11.9.30.7. Conforme o dimensionamento apresentado, serão necessárias 24 licenças da solução Elastic Enterprise. Uma vez que a solução empregada pelo PRODERJ será aquela on-premises, se faz necessário coletar preços de mercado dela. Podem existir custos distintos entre a solução hospedada em nuvem (observada na pesquisa de mercado), em comparação com aquela hospedada localmente.

11.9.31. **Item 24 do Lote III - Serviço técnico especializado para o Licenciamento Elastic Enterprise On-Premises**

11.9.31.1. O Serviço Técnico Especializado para o Licenciamento Elastic Enterprise On-Premises refere-se ao suporte profissional e consultoria oferecidos para a implementação, configuração, otimização e gestão da plataforma Elastic Stack (Elasticsearch, Kibana, Beats, Logstash, APM, Security, etc.) na sua versão Enterprise, instalada e gerenciada dentro da infraestrutura física da sua própria empresa (on-premises).

Este serviço é crucial para organizações que optam por rodar o Elastic Enterprise On-Premises, pois, embora a plataforma seja robusta, sua implementação e otimização são complexas. O serviço serve para:

1) **Implementação e Configuração Otimizada:** Garantir que a Elastic Stack seja instalada e configurada corretamente desde o início, seguindo as melhores práticas para performance, escalabilidade e segurança do seu ambiente. Isso inclui dimensionamento de hardware, otimização de cluster e ajustes de configurações.
2) **Gestão de Licenciamento:** Auxiliar na compreensão dos modelos de licenciamento Enterprise da Elastic, garantindo que a empresa adquira as licenças corretas e as utilize de forma eficiente, evitando custos desnecessários ou infra-licenciamento.
3) **Suporte e Resolução de Problemas:** Oferecer suporte especializado para diagnosticar e resolver problemas que possam surgir, garantindo alta disponibilidade e desempenho da plataforma. Isso é vital para sistemas críticos de observabilidade e segurança.
4) **Customização e Integração:** Ajudar a personalizar a Elastic Stack para atender às necessidades específicas da empresa, seja na integração com outras fontes de dados, na criação de dashboards e relatórios customizados, ou na automação de fluxos de trabalho.
5) **Otimização de Performance:** Realizar análises de performance e aplicar otimizações para garantir que a Elastic Stack processe e analise grandes volumes de dados de forma eficiente, sem comprometer a velocidade das buscas ou a precisão das detecções.
6) **Atualizações e Upgrades:** Gerenciar o processo de atualização e upgrade da Elastic Stack para novas versões, minimizando o tempo de inatividade e garantindo a compatibilidade.
7) **Capacitação da Equipe Interna:** Treinar a equipe de TI da organização para que ela possa gerenciar e operar a plataforma de forma autônoma após a implementação inicial.
8) **Melhoria Contínua:** Fornecer consultoria para aprimorar o uso da Elastic Stack ao longo do tempo, explorando novas funcionalidades (como Machine Learning para casos de uso específicos de segurança ou observabilidade) e adaptando a solução às necessidades de negócios em constante mudança.

11.9.32. **Item 24 do Lote III - Memória de cálculo - UST**

11.9.32.1. Como métrica universal para o consumo de múltiplos serviços correlatos a contratação, os quais contemplam a implantação, a manutenção evolutiva, a manutenção corretiva, a segurança da informação e o treinamento operacional da solução, se determinou a seguir o montante de Unidades de Serviço Técnico dimensionadas em conformidade com a necessidade do PRODERJ.

11.9.32.2. Na memória de cálculo o dimensionamento ponderado levou em consideração a possibilidade de execução de todo o montante de recursos previstos para consumo durante a vigência contratual.

11.9.32.3. Essa quantidade foi empregada como métrica de quantidade na tabela a seguir, exceto nos quantitativos diferentes apresentados, os quais indicam métricas empíricas nossas para consumo ao longo do período contratual.

11.9.32.4. As estimativas utilizadas basearam-se em pesquisas de mercado que demonstram em média **5.082 (cinco mil oitenta e dois) USTs.** para Serviços Técnicos Especializados (sob demanda) durante uma vigência contratual de uma única Unidade Gestora, conforme ANEXO IV - CATÁLOGO DE SERVIÇOS, deste documento.

11.9.32.5. **Memória de cálculo do catálogo de serviços para o Lote III.**

11.9.32.6. **Segue tabela abaixo a estimativa do quantitativo das subatividades relacionadas:**

Complexidade (Baixa, Média ou Alta)	Tipo de Execução (Remoto ou Presencial)	Duração do Serviço (horas)	Validação dos Seviços Executados (horas)	Documentação dos Serviços Executado (Horas)	Total Estimado de Horas	UST AJUSTADA CONFORME A COMPLEXIDADE	QUANTIDADE	TOTAL ESTIMADO
ATIVIDADES DE ARQUITETURA E PROJETO								
BAIXA	REMOTO	6	6	6	18	18	2	36
ALTA	REMOTO	8	7	6	21	31	2	62
MEDIA	REMOTO	6	2	4	12	15	2	30
ALTA	REMOTO	10	7	6	23	34	2	68
MEDIA	REMOTO	4	4	3	11	13	2	26
ALTA	REMOTO	16	7	6	29	43	2	86
MEDIA	REMOTO	6	5	6	17	21	2	42

ALTA	REMOTO	10	3	6	19	28	2	56
ALTA	REMOTO	10	3	6	19	28	2	56
ALTA	REMOTO	10	3	6	19	28	2	56
ALTA	REMOTO	10	3	6	19	28	2	56
MEDIA	REMOTO	6	3	4	13	16	2	32
ALTA	REMOTO	8	6	4	18	27	2	54
ALTA	REMOTO	16	10	8	34	51	2	102
MEDIA	REMOTO	8	8	6	22	27	2	54
MEDIA	REMOTO	8	5	6	19	23	2	46
MEDIA	REMOTO	6	6	4	16	20	2	40
ALTA	REMOTO	24	14	12	50	75	2	150
ALTA	REMOTO	48	40	36	124	186	2	372
ALTA	REMOTO	24	12	8	44	66	2	132
BAIXA	REMOTO	60	8	0	68	68	2	136
MEDIA	REMOTO	24	0	0	24	30	6	180
ATIVIDADES DE MANUTENÇÃO CONTÍNUA								
MEDIA	REMOTO	15	1	1	17	21	3	63
MEDIA	REMOTO	15	1	1	17	21	3	63
MEDIA	REMOTO	4	1	1	6	7	3	21
BAIXA	REMOTO	4	1	1	6	6	3	18
ALTA	REMOTO	6	1	1	8	12	3	36
ALTA	REMOTO	6	1	1	8	12	3	36
MEDIA	REMOTO	4	1	1	6	7	3	21
BAIXA	REMOTO	15	1	1	17	17	3	51
BAIXA	REMOTO	15	1	1	17	17	3	51
ALTA	REMOTO	8	1	1	10	15	3	45
MEDIA	REMOTO	15	1	1	17	21	3	63
ALTA	REMOTO	8	1	1	10	15	3	45
ALTA	REMOTO	8	1	1	10	15	3	45
ALTA	REMOTO	16	1	1	18	27	3	81
ALTA	REMOTO	8	1	1	10	15	3	45
ALTA	REMOTO	12	1	1	14	21	3	63
MEDIA	REMOTO	4	1	1	6	7	3	21
MEDIA	REMOTO	4	1	1	6	7	3	21
ALTA	REMOTO	16	1	1	18	27	3	81
ALTA	REMOTO	4	1	1	6	9	3	27
BAIXA	REMOTO	3	1	1	5	5	3	15
MEDIA	REMOTO	6	1	1	8	10	3	30
ALTA	REMOTO	8	1	1	10	15	3	45
ATIVIDADES ESPECIALIZADAS								

MEDIA	REMOTO	12	1	1	14	17	3	51
ALTA	REMOTO	6	1	1	8	12	3	36
ALTA	REMOTO	24	1	1	26	39	2	78
ALTA	REMOTO	16	1	1	18	27	3	81
ALTA	REMOTO	36	1	1	38	57	2	114
MEDIA	REMOTO	40	1	1	42	52	6	312
ALTA	REMOTO	48	1	1	50	75	3	225
ALTA	REMOTO	12	1	1	14	21	6	126
ALTA	REMOTO	48	1	1	50	75	3	225
ALTA	REMOTO	24	1	1	26	39	3	117
MEDIA	REMOTO	12	1	1	14	17	6	102
MEDIA	REMOTO	15	1	1	17	21	36	756
TOTAL DE USTS								**5.082**

12. **ESTIMATIVA PRELIMINAR DO VALOR DA CONTRATAÇÃO**

12.1. Projetos similares realizados por outros órgãos da Administração Pública, foi realizada a pesquisa no catálogo de soluções de TIC da secretaria de governo digital da secretaria especial de desburocratização gestão e governo digital do ME e não encontramos contratações similares no referido Catálogo de Soluções de TIC.

12.2. O valor estimado para esta contratação é de R$ **37.707.127,34** (trinta e sete milhões, setecentos e sete mil cento e vinte e sete reais e trinta e quatro centavos), baseado nas tabelas do item "**Custo de Propriedade"**, conforme descrito abaixo:

LOTE I				
ITEM	**DESCRIÇÃO**	**QUANTIDADE ESTIMADA**	**VALOR MÉDIO UNITÁRIO**	**VALOR MÉDIO GLOBAL**
1	Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, com Instalação da Solução.	02	R$ 4.270.283,24	**R$ 8.540.566,48**
2	Serviço de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	6.080	R$ 426,18	**2.591.174,40**
3	Treinamento da Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	01	R$ 20.778,74	**R$ 20.778,74**
LOTE II				
4	Equipamento para a interceptação do tráfego.	02	R$ 276.650,66	**R$ 553.301,32**
5	Licenciamento de desduplicação do tráfego.	02	R$ 119.021,58	**R$ 238.043,16**
6	Licenciamento avançado de descriptação do tráfego.	02	R$ 4.160.740,30	**R$ 8.231.480,60**
7	Licenciamento avançado de análise de aplicações.	02	R$ 70.684,64	**R$ 141.369,28**
8	Licenciamento avançado de análise de análise de metadados.	02	R$ 329.696,64	**R$ 659.393,28**
9	Módulo de expansão do processamento.	02	R$ 510.730,00	**R$ 1.021.460,00**
10	Módulo de expansão para a captura do tráfego “inline”.	02	R$ 277.393,76	**R$ 554.787,52**

11	Licenciamento para o gerenciamento centralizado da solução.	01	R$ 383.652,46	**R$ 767.304,92**
12	Interceptador do tráfego virtualizado avançado.	01	R$ 882.161,28	**R$ 882.161,28**
13	Chassi para interconector passivo de interceptação do tráfego - interfaces ópticas	04	R$ 3.833,25	**R$ 15.333,00**
14	Interconector passivo de interceptação do tráfego – interfaces SFP	04	R$ 10.126,56	**R$ 40.506,24**
15	Interconector passivo de interceptação do tráfego – interfaces QSFP	04	R$ 41.569,76	**R$ 166.279,04**
16	Interconector passivo de interceptação do tráfego – interfaces RJ-45	04	R$ 13.825,76	**R$ 55.303,04**
17	Concentrador de Tráfego de Segurança.	01	R$ 323.633,76	**R$ 323.633,76**
18	Transceiver tipo 1 – 1 Gbps ethernet	08	R$ 3.287,66	**R$ 26.301,28**
19	Transceiver tipo 2 – 10 Gbps ethernet	08	R$ 11.573,82	**R$ 92.590,56**
20	Transceiver tipo 3 – 25 Gbps ethernet	08	R$ 5.106,04	**R$ 40.848,32**
21	Transceiver tipo 4 – 100 Gbps ethernet	08	R$ 19.441,88	**R$ 155.535,04**
22	Serviço técnico especializado para a solução de interceptação de tráfego.	3.238	R$ 426,18	**R$1.379.970,84**
LOTE III				
23	Licenciamento Elastic Enterprise On-Premises.	24	R$ 376.798,27	**R$ 9.043.158,48**
24	Serviço técnico especializado para o Licenciamento Elastic Enterprise On-Premises	5.082	R$ 426,18	**R$ 2.165.846,76**
			VALOR GLOBAL DA CONTRAÇÃO	**R$ 37.707.127,34**

13. **DESCRIÇÃO DA SOLUÇÃO COMO UM TODO**

13.1. Contratação de empresas especializadas em soluções de monitoramento de comportamento anômalo da rede, de observabilidade e otimização de tráfego de rede e análise, indexação e visualização de dados de rede e eventos de segurança para suporte à detecção e resposta a incidentes, contemplando hardware, software, implantação e treinamento com garantia do fabricante por 36 (trinta e seis) meses.

14. **NATUREZA DO OBJETO DA CONTRATAÇÃO**

14.1. Trata-se de objeto composto por bens e serviços de ***natureza comum***, nos termos do parágrafo único, do art. 6º, XIII, da Lei nº 14.133/2021, uma vez que os seus padrões de desempenho e qualidade encontram-se objetivamente definidos no edital, por meio de especificações usuais no mercado.

14.2. A prestação de serviços será de ***natureza continuada***, pois visa atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público e o funcionamento das atividades do órgão ou entidade, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional.

14.3. Os itens referentes aos treinamentos e aos Serviços Técnicos Especializados, embora executados sob demanda, também possuem natureza continuada, tendo em vista a necessidade de disponibilidade permanente do serviço durante a operação dos serviços de subscrição, para atendimento às solicitações do órgão contratante sempre que necessário.

14.4. O item 1 do Lote I e os itens 4, 9, 10, 13, 14, 15, 16, 17, 18, 19, 20 e 21 do Lote II são aquisição de bens comuns.

14.5. Os itens 2 do Lote I, os itens 5, 6, 7, 8, 11, 12 e 22 do Lote II; e itens 23 e 24 do Lote III são serviços comuns de natureza continuada.

15. **JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO**

15.1. O parcelamento da solução em lotes, conforme apresentado na tabela, é uma estratégia que busca otimizar a contratação pública, alinhando-se aos princípios da economicidade, da busca pela proposta mais vantajosa para a administração e da ampliação da competitividade.

15.2. Apresentamos a justificativa para essa divisão:

15.2.1. **Separação de Bens e Serviços Essenciais da Solução Principal (Lote I)**

15.2.1.1. O Lote I concentra a Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação (NDR), juntamente com seu serviço de instalação e treinamento. Essa é a essência da contratação, o "core" do que se pretende adquirir.

- Vantagem: Ao isolar a solução principal, a Administração pode focar na busca por um fornecedor que seja especialista na tecnologia NDR e que ofereça a melhor solução em termos de funcionalidade, desempenho e segurança, com a garantia e suporte direto do fabricante. Isso evita que a complexidade de outros itens dilua a avaliação da tecnologia central.

15.3. **Agrupamento de Componentes de Infraestrutura e Licenciamentos Necessários (Lote II)**

15.3.1. O Lote II agrupa todos os equipamentos e licenciamentos acessórios que são cruciais para o funcionamento e a otimização da solução de interceptação do tráfego, além do serviço técnico especializado para sua instalação, configuração e monitoramento. Inclui itens como equipamentos de interceptação de tráfego, diversos tipos de licenciamentos avançados (desduplicação, descriptografia, análise de aplicações e metadados), módulos de expansão e concentradores de tráfego.

- Vantagem: A consolidação desses itens em um lote separado permite que a Administração busque um fornecedor que seja competitivo em hardware e licenciamentos complementares, e que tenha a expertise para integrar esses componentes as soluções de segurança que receberão tráfego do PRODERJ. Além disso, ao agrupar serviços técnicos especializados relacionados a esses componentes, garante-se uma responsabilidade clara pela sua operação e suporte.

15.4. **Aquisição de Plataforma de Dados e Serviço Associado (Lote III)**

15.4.1. O Lote III destina-se ao Licenciamento Elastic Enterprise On-Premises e seu serviço técnico especializado. A plataforma Elastic é amplamente utilizada para coleta, armazenamento, análise e visualização de grandes volumes de dados (como os gerados pela solução NDR), sendo um componente de infraestrutura de dados essencial para o funcionamento eficaz da análise de comportamento anômalo.

- Vantagem: A separação deste lote permite que a Administração contrate um fornecedor especializado na plataforma Elastic, que pode não ser o mesmo fornecedor da solução NDR ou dos componentes de infraestrutura de rede. Empresas com expertise em soluções de Big Data e análise podem oferecer melhores condições e maior qualidade na implementação e suporte do Elastic. Isso garante que a plataforma de dados, vital para a inteligência da solução, seja dimensionada e configurada de forma ótima, aproveitando o conhecimento de especialistas nesse domínio.

15.5. **Benefícios Gerais do Parcelamento:**

- Ampla Competitividade: Permite que diferentes tipos de empresas (especializadas em NDR, em hardware de rede, em soluções de dados) participem da licitação para os lotes que se encaixam em sua expertise, aumentando o número de concorrentes e, consequentemente, a chance de se obter propostas mais vantajosas.
- Melhor Adequação Técnica: Facilita a contratação de fornecedores que são verdadeiros especialistas em cada componente da solução, garantindo a qualidade técnica e a otimização de cada parte do sistema.
- Otimização de Preços: A competição em lotes específicos tende a gerar preços mais competitivos para cada um dos grupos de itens, resultando em uma economia global para a Administração.
- Gestão Contratual Simplificada (por especialidade): Embora haja mais contratos, a gestão se torna mais focada em cada área de especialidade, facilitando a fiscalização e o acompanhamento da execução.

15.5.1. Em suma, o parcelamento em lotes é uma estratégia que visa a eficiência e a economicidade, garantindo que cada componente da complexa solução de segurança cibernética seja adquirido e implementado com a melhor qualidade e o custo mais adequado, através da competição e especialização do mercado.

Solução de interceptação de tráfego, monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, incluindo hardware, software e demais componentes, bem como treinamento e garantia com manutenção do fabricante por 36 (trinta e seis) meses.				
LOTE I				
ITEM	**DESCRIÇÃO**	**MÉTRICA**	**FORMA DE FORNECIMENTO**	**QUANTIDADE ESTIMADA**
1	Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, com Instalação da Solução.	Unidade	Aquisição	02
2	Serviço técnico especializado de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	UST	Sob Demanda	6.080
3	Treinamento da Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	Turma	Sob Demanda	01
LOTE II				
4	Equipamento para a interceptação do tráfego	Unidade	Aquisição de Equipamento	02
5	Licenciamento de desduplicação do tráfego.	Unidade	Subscrição de Licença por 36 meses	02
6	Licenciamento avançado de descriptação do tráfego.	Unidade	Subscrição de Licença por 36 meses	02

7	Licenciamento avançado de análise de aplicações.	Unidade	Subscrição de Licença por 36 meses	02
8	Licenciamento avançado de análise de análise de metadados.	Unidade	Subscrição de Licença por 36 meses	02
9	Módulo de expansão do processamento.	Unidade	Aquisição de Equipamento	02
10	Módulo de expansão para a captura do tráfego “inline”.	Unidade	Aquisição de Equipamento	02
11	Licenciamento para o gerenciamento centralizado da solução.	Unidade	Subscrição de Licença por 36 meses	01
12	Interceptador do tráfego virtualizado avançado.	Unidade	Subscrição de Licença por 36 meses	01
13	Chassi para interconector passivo de interceptação do tráfego - interfaces ópticas	Unidade	Aquisição de Equipamento	04
14	Interconector passivo de interceptação do tráfego – interfaces SFP	Unidade	Aquisição de Equipamento	04
15	Interconector passivo de interceptação do tráfego – interfaces QSFP	Unidade	Aquisição de Equipamento	04
16	Interconector passivo de interceptação do tráfego – interfaces RJ-45	Unidade	Aquisição de Equipamento	04
17	Concentrador de Tráfego de Segurança.	Unidade	Aquisição de Equipamento	01
18	Transceiver tipo 1 – 1 Gbps ethernet	Unidade	Aquisição de Equipamento	08
19	Transceiver tipo 2 – 10 Gbps ethernet	Unidade	Aquisição de Equipamento	08
20	Transceiver tipo 3 – 25 Gbps ethernet	Unidade	Aquisição de Equipamento	08
21	Transceiver tipo 4 – 100 Gbps ethernet	Unidade	Aquisição de Equipamento	08
22	Serviço técnico especializado para a solução de interceptação de tráfego.	UST	Sob Demanda	3.238
LOTE III				
23	Licenciamento Elastic Enterprise On-Premises.	Unidade	Subscrição de Licença por 36 meses	24
24	Serviço técnico especializado para o Licenciamento Elastic Enterprise On-Premises.	UST	Sob Demanda	5.082

16. **DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS**

16.1. A presente contratação tem por objetivo obter soluções de monitoramento de comportamento anômalo da rede, de observabilidade e otimização de tráfego de rede e análise, indexação e visualização de dados de rede e eventos de segurança para suporte à detecção e resposta a incidentes, contemplando hardware, software, implantação e treinamento com garantia do fabricante por 36 (trinta e seis) meses.

16.2. Espera-se com a inovação tecnológica proposta no presente documento, obter, ainda, os seguintes resultados:

a) Proteger sites e aplicações WEB contra ameaças de segurança;

b) Aumentar economia de banda e infraestrutura, com filtragem e redirecionamento de tráfego, bem como mitigação de ataques, bem como suas tentativas, que consomem tráfego de internet, infraestrutura e recursos operacionais;

c) Melhorar as ações de segurança da informação da Administração Pública;

d) Aumentar o grau de confidencialidade da segurança da informação;

e) Elevar a integridade e segurança de dados;

f) Assegurar o provimento de Infraestrutura de TI segura e adequada para que as áreas finalísticas do negócio mantidas pela Administração Pública continuem operacionais;

g) Contribuir para a garantia da disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;

h) Evitar que os serviços prestados fiquem indisponíveis por esgotamento da capacidade de transporte de dados na rede e por ataques cibernéticos; e

i) Prevenir e minimizar o impacto de incidentes.

17. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

17.1. O CONTRATANTE indicará servidores para desempenhar os papéis de gestor do contrato, fiscal técnico, fiscal da área requisitante e fiscal administrativo, bem como os respectivos suplentes para esta contratação.

17.2. Não haverá necessidade de capacitação dos servidores que farão a gestão e fiscalização dos serviços.

18. REQUISITOS DE QUALIFICAÇÃO TÉCNICA

18.1. Comprovação de aptidão para a prestação de serviços, de acordo com as características, quantidades e prazos compatíveis com o objeto, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, na seguinte forma:

18.2. Para o LOTE I: O(s) atestado(s) deverão demonstrar o fornecimento de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação (item 1), correspondente a aproximadamente 33,33% do quantitativo total estimado do item 1.

18.2.1. Para o LOTE II: O(s) atestado(s) deverão demonstrar o cumprimento de um quantitativo no mínimo de, ao menos, 1 (uma) unidade de interceptação de tráfego composta por módulos físicos (Item 4) ou virtuais da solução (Item 12), independentemente do modelo de licenças ou licenciamento empregado nela, correspondente a aproximadamente 33,33% do quantitativo total estimado) dos itens 4 e 12.

18.2.2. Para o LOTE III: O(s) atestado(s) deverão demonstrar o cumprimento de um quantitativo no mínimo de, ao menos, 1 (uma) unidade de licença da solução Elastic Search (Item 23), seja do software ou da sua garantia oficial, correspondente a aproximadamente 5,55% do quantitativo total estimado) do item 23.

18.3. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

18.4. Será admitido, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, resultando na comprovação de capacidade técnico-operacional de uma única contratação.

18.5. Em caso de dúvida fundada suscitada pelo pregoeiro, a Administração poderá solicitar ao licitante, em diligência complementar, todas as informações necessárias à comprovação da legitimidade dos atestados, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

18.6. A motivação se deve à comprovação de aptidão técnica em virtude de se tratar de contratação para atendimento em larga escala, que demanda a necessidade de prestador com capacidade de atendimento compatível com a criticidade do projeto, mitigando riscos à disponibilidade dos serviços do Governo, bem como diante da importância do objeto a ser contratado, que tem relação direta com a segurança institucional da Administração Pública.

19. AMOSTRA, EXAME DE CONFORMIDADE E PROVA DE CONCEITO

19.1. **Prova de Conceito:**

19.1.1. Será necessário realizar verificação por Prova de Conceito do objeto para averiguar se detém os requisitos mínimos de acordo com as caracterísitcas, funcionalidades, procedimentos e critérios descritos nos anexos III e IV deste estudo.

19.1.2. Será exigida Prova de Conceito dos Lotes I e II, considerando a necessidade de validação prática da aderência das soluções aos requisitos funcionais e técnicos estabelecidos neste Estudo.

19.1.3. Para o Lote III, a Prova de Conceito não será exigida, tendo em vista que requisitos técnicos do objeto são objetivos, padronizados e passíveis de verificação por meio de documentação técnica oficial do fabricante, tais como encartes técnicos, *datasheets*, manuais e demais especificações formais, suficientes para comprovar o atendimento integral às exigências estabelecidas, sem necessidade de demonstração prática.

19.1.4. Se a licitante convocada deixar de comparecer no dia designado para realização da prova de conceito sem justificativa aceita pelo pregoeiro, ou havendo incompatibilidade da solução com as especificações técnicas exigidas no edital, a proposta do licitante será recusada.

19.1.5. Se a Solução apresentada pelo primeiro classificado não for aceita, os integrantes técnicos da equipe de planejamento analisarão a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da Solução e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Anexo I.

19.1.6. A prova de conceito consistirá na apresentação do funcionamento do objeto, conforme especificações constantes do Anexo I - Especificações Técnicas do Objeto (127234752).

20. POSSIBILIDADE DE SUBCONTRATAÇÃO

20.1. Não será admitida subcontratação, tendo em vista a indivisibilidade técnica e operacional do objeto, cuja eficácia depende da integração plena entre os componentes da solução (plataforma, suporte técnico e capacitação), todos sob responsabilidade direta e contínua do mesmo fornecedor. A subcontratação parcial comprometeria o controle, a rastreabilidade e a segurança na execução, contrariando os princípios da eficiência e da mitigação de riscos que regem a presente contratação.

21. POSSIBILIDADE DE PARTICIPAÇÃO DE MICROEMPRESAS, PEQUENAS EMPRESAS E EMPRESÁRIOS INDIVIDUAIS

21.1. Não será aplicada reserva de cota para microempresas, empresas de pequeno porte ou empresários individuais, tendo em vista a natureza indivisível do objeto licitado. A Solução de interceptação de tráfego, monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, incluindo hardware, software e demais componentes, bem como treinamento e garantia com manutenção do fabricante por 36 (trinta e seis) meses.

21.2. Essa característica inviabiliza sua divisão em partes autônomas para adjudicação parcial a diferentes fornecedores, que admitem a não aplicação das regras de favorecimento a ME/EPP quando o objeto for tecnicamente indivisível ou exigir execução integrada e padronizada.

21.3. Ressalta-se ainda que não foram identificados, no levantamento de mercado, fornecedores de pequeno porte que, isoladamente, reúnam as condições técnicas, organizacionais e de certificação exigidas para a prestação integral do objeto com a robustez necessária, o que poderia implicar risco à segurança institucional e à continuidade dos serviços públicos críticos prestados pelo PRODERJ.

22. POSSIBILIDADE DE PARTICIPAÇÃO DE CONSÓRCIOS E COOPERATIVAS

22.1. Participação de Consórcios

22.1.1. A vedação à participação de interessadas que se apresentem constituídas em consórcio se justifica na medida em que nas licitações que visam à contratação de bens e serviços de TIC, existem no mercado empresas em quantidade e capacidade técnica suficientes para garantir um processo altamente competitivo e executar o objeto sem, necessariamente, se consorciar a outras empresas. A ausência de consórcio não trará prejuízos à competitividade do certame.

22.1.2. A importância de ser uma única empresa responsável em cada Lote, guarda relação com o gerenciamento dos dados, evita a fragilidade das informações trazendo maior segurança dos processos. Portanto, não será permitida a participação de empresas que estiverem reunidas em consórcio, qualquer que seja sua forma de constituição. Em regra, a formação de consórcios é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital. Nestes casos, a Administração, com vistas a aumentar o número de participantes, admite a formação de consórcio.

22.2. Participação de Cooperativas

22.2.1. A participação de Cooperativas será permitida observando às obrigações do Art. 16 da Lei 14.133/21:

> *"Art. 16. Os profissionais organizados sob a forma de cooperativa poderão participar de licitação quando:*
>
> *I - a constituição e o funcionamento da cooperativa observarem as regras estabelecidas na legislação aplicável, em especial a Lei nº 5.764, de 16 de dezembro de 1971, a Lei nº 12.690, de 19 de julho de 2012, e a Lei Complementar nº 130, de 17 de abril de 2009;*
>
> *II - a cooperativa apresentar demonstrativo de atuação em regime cooperado, com repartição de receitas e despesas entre os cooperados;*
>
> *III - qualquer cooperado, com igual qualificação, for capaz de executar o objeto contratado, vedado à Administração indicar nominalmente pessoas;*
>
> *IV - o objeto da licitação referir-se, em se tratando de cooperativas enquadradas na Lei nº 12.690, de 19 de julho de 2012, a serviços especializados constantes do objeto social da cooperativa, a serem executados de forma complementar à sua atuação."*

23. PRAZO DO CONTRATO E POSSIBILIDADE DE PRORROGAÇÃO

23.1. O prazo de vigência do contrato relativo ao fornecimento do item 1 do lote I, e dos itens 4, 9, 10, 13 a 21 do lote II serão de 180 (cento e oitenta) dias, contados da data da divulgação no Portal Nacional de Contratações Públicas.

23.2. O prazo de vigência de 180 (cento e oitenta) dias será automaticamente prorrogado, sem prejuízo da formalização adequada, quando o objeto não for concluído no período firmado acima, ressalvadas as providências cabíveis no caso de culpa do contratado, previstas neste instrumento e no Contrato, nos termos do art. 111 da Lei n° 14.133/2021

23.3. O prazo de vigência do contrato referente a garantia do item 1 do lote I, e dos itens 4, 9, 10, 13 a 21 do lote II será de 36 (trinta e seis) meses, a contar do recebimento definitivo dos itens.

23.4. O prazo de vigência do Contrato relativo aos serviços dos itens 5, 6, 7, 8, 11, 12 do lote II e 23 do lote III - que tratam de Subscrição, o item 3 do lote I que trata de treinamento, o item 2 lote I, item 22 do lote II e o item 24 do lote III que tratam dos Serviços Técnicos Especializados será de 36 (trinta e seis) meses, contado da data da divulgação no Portal Nacional de Contratações Públicas.

23.5. O prazo de vigência do Contrato relativo aos Itens 5, 6, 7, 8, 11, 12 do lote II e 23 do lote III - que tratam de Subscrição, o item 3 do lote I que trata de treinamento e o item 2 lote I, item 22 do lote II e o item 24 do lote III que tratam dos Serviços Técnicos Especializados, poderá ser prorrogado até o máximo de 10 (dez) anos, na forma dos arts. 106 e 107 da Lei n° 14.133/2021, desde que observadas as condições previstas no Contrato, e mediante a celebração de termo aditivo.

24. LOCAL DE ENTREGA DOS BENS OU DA PRESTAÇÃO DO SERVIÇO

24.1. O endereço de entrega dos bens do item 1 do Lote I, item 4 e itens de 13 a 21 do Lote II, (aquisição) será o endereço do CONTRATANTE, que constará na autorização de fornecimento emitida. Os itens deverão ser entregues instalados e configurados.

24.2. As Subscrições das licenças demandadas dos itens de 5 a 8, 11 e 12 do Lote II e para o item 23 do Lote III serão entregues, instaladas e configuradas de uma única vez no ambiente tecnológico do CONTRATANTE;

24.3. Para o serviço de treinamento item 3 do Lote I (treinamento - sob demanda), ocorrerá conforme o item Requisitos de Capacitação deste documento, as demais especificações estão descritas no ANEXO I - ESPECIFICAÇÃO TÉCNICA, deste documento.

24.4. Para o item 2 do Lote I, do item 22 do Lote II e item 24 do Lote III (Serviços Técnicos Especializados) será realizado de forma remota ou presencial, a ser definido pelas partes em reunião de kick-off, conforme especificado no ANEXO I - ESPECIFICAÇÃO TÉCNICA, deste documento.

25. PRAZOS E CONDIÇÕES DE ENTREGA DOS BENS OU DA EXECUÇÃO DOS SERVIÇOS

25.0.1. O prazo de entrega dos objetos para o item 1 do Lote I, itens 4, 9, 10, 13, 14, 15, 16, 17, 18, 19, 20, 21 do Lote II, (aquisição) será de até 90 (noventa) dias corridos a contar da emissão da ordem de fornecimento, que poderá ser emitida após a divulgação do contrato no Portal Nacional de Compras Públicas (PNCP).

25.0.2. O prazo de entrega do objeto para os itens 5, 6, 7, 8, 11 e 12 do Lote II e para o item 23 do Lote III (subscrição de licenças) será de até 30 (trinta) dias corridos a contar da emissão da ordem de serviço, que poderá ser emitida após a divulgação do contrato no Portal Nacional de Compras Públicas (PNCP).

25.1. O prazo de entrega do serviço do item 3 do Lote I (treinamentos) será de até 30 (trinta) dias corridos a contar da emissão da ordem de serviço, que poderá ser emitida após a divulgação do contrato no Portal Nacional de Compras Públicas (PNCP), após a entrega do item de 1 do lote I.

25.2. O prazo de entrega item 2 do Lote I, do item 22 do Lote II e item 24 do Lote III (Serviços Técnicos Especializados), com medição em UST terão os prazos de entrega definidos nas respectivas Ordens de de serviço, que poderão ser emitidas após a divulgação do contrato no Portal Nacional de Compras Públicas (PNCP).

26. METODOLOGIA DE AVALIAÇÃO DA QUALIDADE E ACEITE DO OBJETO EXECUTADO (ANS)

26.1. Para os itens 1 do Lote I e itens 4, 9, 10, 13, 14, 15, 16, 17, 18, 19, 20, 21 do Lote II, que são os de aquisição, o Acordo de Nível de Serviço será aquele definido pelo fabricante da solução ofertada, nos termos e condições de uso oficialmente disponibilizadas no site oficial.

26.2. Para os itens de serviços técnicos especializados, cuja execução se dará por meio de Ordens de Serviço e o pagamento sob demanda, a avaliação da qualidade e o aceite do objeto ocorrerão mediante inspeção do fiscal técnico no recebimento provisório e definitivo, conforme o item "Regras para o recebimento provisório e definitivo", dispensando-se o monitoramento.

- **Finalidade:** Garantir a qualidade do Suporte Técnico do objeto.
- **Periodicidade:** Bimestral.
- **Início da medição:** A partir do 2º mês após a plena instalação e configuração da solução tecnológica. (item 1, itens de 4 a 21 e item 23)
- **Mecanismo de cálculo:** Somatório dos índices correspondentes aos eventos previstos nas alíneas "a, b, c, d" do subtópico 26.19 deste documento, verificados durante o período.

26.3. A contratada deverá cumprir prazos máximos para respostas aos acionamentos, de acordo com o nível de severidade de cada chamado, bem como os prazos de atendimento, conforme o quadro abaixo:

ATENDIMENTO			
Severidade	**Tempo máximo para início de atendimento**	**Tempo máximo para solução operacional**	**Grau de cumprimento**
CRÍTICO	Em até 30min	Em até 4 horas	95%
ALTA	Em até 1 hora	Em até 12 horas	95%
MÉDIA	Em até 2 horas	Em até 48h	90%
BAIXA	Em até 24 horas	Em até 72h	85%

26.4. A disponibilidade da ferramenta deve ser de 99,5% durante a vigência do contrato (cerca de 44 horas de indisponibilidade ao ano), caso o tempo de indisponibilidade ultrapasse o definido será considerada como severidade CRÍTICA.

26.5. O nível de severidade será informado pelo Contratante no momento da abertura do chamado, podendo ser reclassificado a critério do Contratante, caso em que ocorrerá início de nova contagem de prazo para o seu cumprimento.

26.6. O chamado não atendido no prazo estabelecido poderá ser reaberto, classificado no nível de severidade imediatamente superior, independentemente da aplicação das sanções aqui previstas.

26.7. O descumprimento deste acordo de nível de serviço, notadamente quanto ao cumprimento dos prazos, ensejará as sanções previstas no subtópico 26.19 deste documento.

26.8. Forma de atendimento: Os trabalhos deverão ser desenvolvidos por técnicos e consultores capacitados e certificados da CONTRATADA, através de instruções telefônicas, tele presenciais e presenciais para solução de problemas e operação dos componentes tecnológicos ou da intervenção remota através da Internet, utilizando para isto de ferramentas que garantam a confidencialidade das informações;

26.9. Tempo de resposta: Os atendimentos deverão ser respondidos e classificados em um prazo compatível com o nível de urgência especificado no momento da abertura do chamado ou identificação da anomalia e iminência de exploração, conforme descrito na tabela do subtópico

26.10. Tempo de solução: o tempo de solução de problemas dependerá de sua extensão, gravidade, disponibilidade e risco à disponibilidade ou integridade aos ativos da instituição. A CONTRATADA deverá fornecer uma estimativa de tempo para solução do problema dentro da primeira hora de atendimento.

26.11. Atendimento no local: Nos casos, classificados em grau de severidades Crítico/Alta, em que a intervenção remota não for efetiva, ou seja, após decorrido o prazo da estimativa de tempo fornecido para a solução do problema, a CONTRATADA deverá imediatamente, às suas custas, deslocar um técnico com o perfil necessário para atender ao problema em no máximo até 24 (vinte e quatro horas).

26.12. O técnico da CONTRATADA deverá apresentar, no ato do atendimento, credenciamento (crachá da empresa) e documento de identidade pessoal (RG), para efetuar qualquer serviço.

26.13. Informar à CONTRATANTE, quando da assinatura do contrato, as credenciais para acompanhamento de chamados junto ao fabricante oficial da solução. Este acompanhamento de chamados de suporte com o fabricante da solução deverá ser através da web ou via telefone 0800 do fabricante, sem ônus financeiros adicionais para o CONTRATANTE.

26.14. Caso sejam constatados problemas com a solução fornecida, tais como: mau funcionamento, erros de codificação, ou outras condições que impeçam/atrapalhem a execução das atividades dos usuários ou administradores da solução ofertada, que a CONTRATADA não consiga solucionar ou que extrapole seu campo de ação e conhecimento, deverá esta abrir chamado direto com o fabricante oficial da solução ofertada para tratamento do problema.

26.15. A Comissão de Fiscalização do Contrato a cada dois meses de apuração, deverá comunicar à Contratada o resultado da apuração.

26.16. A comunicação poderá ser feita pessoalmente, ou por meio eletrônico.

26.17. A CONTRATADA deverá enviar bimestralmente relatório resumido dos atendimentos eventualmente realizados no período.

26.18. O prazo para substituição de módulos que apresentarem qualquer tipo de falha ou defeito durante a execução contratual será de 1 (um) dia útil.

26.19. **Sanções**

26.19.1. Ocorrerá aplicação de multas por motivo de descumprimento deste Acordo de Nível de Serviços, conforme os valores a seguir:

a) 0,10% do valor anual da solução a título de multa, por 10% de demandas categorizadas como "BAIXA" não atendidas no prazo, observados os limites quanto ao início do atendimento e solução operacional.

b) 0,20% do valor anual da solução a título de multa, por 5% de demandas categorizadas como “MÉDIA” não atendidas no prazo, dentro do período de apuração, observados os limites quanto ao início do atendimento e solução operacional.

c) 0,30% do valor anual da solução a título de multa, por 3% de demandas categorizadas como “ALTA” não atendidas no prazo, dentro do período de apuração, observados os limites quanto ao início do atendimento e solução operacional.

d) 0,50% do valor anual da solução a título de multa, por 1% de demandas categorizadas como “CRÍTICA” não atendidas no prazo, dentro do período de apuração, observados os limites quanto ao início do atendimento e solução operacional.

26.19.2. Os descontos relativos à redução por não cumprimento do nível de serviço não serão aplicados para demandas não rotineiras, no caso, por exemplo, de novas instalações;

26.19.3. Qualquer descumprimento do nível de serviço mínimo exigido poderá implicar a aplicação da legislação licitatória quanto à inexecução e à rescisão dos contratos;

26.19.4. Ficam resguardadas as demais sanções previstas em lei conforme o Edital.

27. CRITÉRIOS DE MEDIÇÃO, DE PAGAMENTO E FORMA DE REAJUSTAMENTO DO CONTRATO

27.1. Reajuste de Preços

27.1.1. Os preços contratados serão reajustados após o interregno de 1 (um) ano, mediante solicitação do CONTRATADO.

27.1.2. O interregno mínimo de 1 (um) ano para o primeiro reajuste será contado da data do orçamento estimado.

27.1.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir do fato gerador que deu ensejo ao último reajuste.

27.1.4. Os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do Índice de Custos de Tecnologia da Informação – ICTI, exclusivamente para as obrigações que se iniciem após a anualidade.

27.1.5. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, o CONTRATANTE pagará ao CONTRATADO a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

27.1.6. Fica o CONTRATADO obrigado a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer, sendo adotado na aferição final o índice definitivo.

27.1.7. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

27.1.8. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

27.1.9. O pedido de reajuste deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação contratual, sob pena de preclusão.

27.1.10. Os efeitos financeiros do pedido de reajuste serão contados:

a) Da data-base prevista no contrato, desde que requerido o reajuste no prazo de 60 (sessenta) dias da data de publicação do índice ajustado contratualmente;

b) A partir da data do requerimento do CONTRATADO, caso o pedido seja formulado após o prazo fixado na alínea a, acima, o que não acarretará a alteração do marco para cômputo da anualidade do reajustamento, já adotado no edital e no contrato.

27.1.11. Caso, na data de eventual prorrogação contratual, ainda não tenha sido divulgado o índice de reajuste, deverá, a requerimento do CONTRATADO, ser inserida cláusula no termo aditivo de prorrogação para resguardar o direito futuro do CONTRATADO, a ser exercido tão logo se disponha dos valores reajustados, sob pena de preclusão.

27.1.12. A extinção do contrato não configurará óbice para o deferimento do reajuste solicitado tempestivamente, hipótese em que será concedido por meio de termo indenizatório.

27.1.13. O reajuste será realizado por apostilamento, se esta for a única alteração contratual a ser realizada.

27.1.14. O reajuste de preços não interfere no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 124, inciso II, alínea “d”, da Lei n.º 14.133/2021.

27.2. **De Pagamento**

27.2.1. O CONTRATANTE deverá pagar o preço, diretamente na conta-corrente de titularidade do CONTRATADO a ser indicada, junto à instituição financeira contratada pelo Estado do Rio de Janeiro, da seguinte forma:

a) Em 1 (uma) paracela, a vista, de acordo com cada ordem de serviço, para os seguintes itens: - Item 1 do Lote 1 (aquisição); - Itens 4, 9, 10, 13, 14, 15, 16, 17, 18, 19, 20, 21 do Lote II (aquisição); - Itens 5, 6, 7, 8, 11 e 12 do Lote II (subscrição) e Item 23 do Lote III (subscrição).

b) Parcelado, sob demanda, de acordo com cado ordem de serviço, para os seguintes itens: - Item 3 do Lote I (treinamento - sob demanda); - Item 2 do Lote I (Serviço Técnico Especializado - sob demanda), - Item 22 do Lote II (Serviço Técnico Especializado - sob demanda) e Item 24 do Lote III (Serviço Técnico Especializado - sob demanda).

27.2.2. No caso de o CONTRATADO estar estabelecido em localidade que não possua agência da instituição financeira contratada pelo Estado do Rio de Janeiro ou, caso verificada pelo CONTRATANTE a impossibilidade de o CONTRATADO, em razão de negativa expressa da instituição financeira contratada pelo Estado do Rio de Janeiro, abrir ou manter conta- corrente naquela instituição financeira, o pagamento poderá ser feito mediante crédito em conta-corrente de outra instituição financeira. Nesse caso, eventuais ônus financeiros e/ou contratuais adicionais serão suportados exclusivamente pelo CONTRATADO.

27.2.3. A emissão da Nota Fiscal ou Fatura será precedida do recebimento definitivo do objeto ou de cada parcela, mediante atestação, que não poderá ser realizada pelo ordenador de despesas, conforme disposto neste instrumento e/ou no Termo de Referência, bem ainda no artigo 140, II, alínea “b”, da Lei nº 14.133/2021 e arts. 20 e 22, XXIII, do Decreto nº 48817/2023.

27.2.4. Quando houver glosa parcial do objeto, o CONTRATANTE deverá comunicar ao CONTRATADO para que emita Nota Fiscal ou Fatura com o valor exato dimensionado.

27.2.5. O CONTRATADO deverá encaminhar a Nota Fiscal ou Fatura para pagamento à CONTRATANTE para o endereço eletrônico a ser indicado.

27.2.6. Uma vez recebidos os documentos mencionados no item Requisitos de qualificação técnica deste documento, o órgão competente deverá verificar:

a) a manutenção das condições de habilitação exigidas pelo instrumento convocatório;

b) se o contratado foi penalizado com as sanções de declaração de inidoneidade ou impedimento de licitar e contratar com o poder público mediante consulta aos cadastros oficiais do poder público existentes, observadas as abrangências de aplicação; e

c) por consulta ao SICAF, eventuais ocorrências impeditivas indiretas, hipótese na qual o gestor deverá verificar se houve fraude por parte das empresas apontadas ao Relatório de Ocorrências Impeditivas Indiretas.

27.2.7. Constatando-se a situação de irregularidade do CONTRATADO, será providenciada sua notificação, por escrito, para que, no prazo de 15 (quinze) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa e especifique provas que pretende produzir. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CONTRATANTE.

27.2.8. Não havendo regularização ou sendo a defesa considerada improcedente, o CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do CONTRATADO, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

27.2.9. Persistindo a irregularidade, o CONTRATANTE deverá adotar as medidas necessárias à rescisão do Contrato nos autos do processo administrativo correspondente, assegurada ao CONTRATADO a ampla defesa.

27.2.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do Contrato, caso o CONTRATADO não regularize sua situação.

27.2.11. O pagamento será efetuado no prazo máximo de até 30 (trinta) dias, contados do recebimento da Nota Fiscal ou Fatura.

27.2.12. Havendo erro na apresentação da Nota Fiscal ou Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que o CONTRATADO providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

27.2.13. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

27.2.14. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

27.2.15. O CONTRATADO regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele Regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar nº 123/2006.

27.2.16. Os pagamentos eventualmente realizados com atraso, desde que não decorram de ato ou fato atribuível ao CONTRATADO, sofrerão a incidência de atualização monetária e juros de mora pelo IPCA-E, calculado pro rata die, e aqueles pagos em prazo inferior ao estabelecido no instrumento convocatório serão feitos mediante desconto de 0,5% (um meio por cento) ao mês, calculado pro rata die.

27.2.17. O CONTRATADO deverá emitir a Nota Fiscal Eletrônica – NF-e, consoante o Protocolo ICMS nº 42/2009, com a redação conferida pelo Protocolo ICMS nº 85/2010, e caso seu estabelecimento esteja localizado no Estado do Rio de Janeiro, deverá observar a forma prescrita nas alíneas a, b, c, d e e, do §1º, do art. 2º da Resolução SEFAZ nº 971/2016.

27.2.18. Caso o CONTRATADO não esteja aplicando o regime de cotas na forma da Lei estadual nº 7.258, de 12 de abril de 2016, deste edital e do contrato, suspender-se-á o pagamento devido, até que seja sanada a irregularidade apontada pelo órgão de fiscalização do Contrato.

27.3. **Regime de execução**

27.3.1. *Para aquisição de bens comuns: item 1 do Lote I, e para os itens 4, 9, 10, 13, 14, 15, 16, 17, 18, 19, 20, 21 do Lote II, será de Entrega Imediata e Integral (inciso X do art. 6º da Lei n. 14.133/2021);*

27.3.2. *Para contratação dos serviços comuns de natureza continuada: itens 2, 3 do Lote I; itens 5, 6, 7, 8, 11, 12 e 22 do Lote II; e itens 23 e 24 do Lote III, será de empreitada por preço unitário (inciso XXVIII do art. 6º da Lei n. 14.133/2021);*

28. **REGRAS PARA O RECEBIMENTO PROVISÓRIO E DEFINITIVO**

28.1. O objeto do contrato será recebido, na seguinte forma:

28.1.1. Para o item 1 do Lote I, para os itens 4, 9, 10, 13, 14, 15, 16, 17, 18, 19, 20, 21 do Lote II - Aquisição equipamentos - (redação do art. 20, II, do Decreto 48.817/23):

a) provisoriamente, pelos fiscais dos contratos, mediante termo, no prazo de 15 (quinze) dias corridos após a entrega dos serviços, quando verificado o cumprimento das exigências de caráter técnico;

b) definitivamente, mediante parecer circunstanciado da comissão de fiscalização, após decorrido o prazo de 30 (trinta) dias corridos do recebimento provisório, para observação e vistoria, que comprove o exato cumprimento das obrigações contratuais;

28.1.2. Para os itens de 5, 6, 7, 8, 11 e 12 do Lote II e item 23 do Lote III - Subscrição - (redação do art. 20, I, do Decreto 48.817/23):

a) provisoriamente, pelos fiscais dos contratos, mediante termo, no prazo de 15 (quinze) dias corridos após a entrega dos serviços, quando verificado o cumprimento das exigências de caráter técnico;

b) definitivamente, mediante parecer circunstanciado da comissão de fiscalização, após decorrido o prazo de 30 (trinta) dias corridos do recebimento provisório, para observação e vistoria, que comprove o exato cumprimento das obrigações contratuais;

28.1.3. Para o item 3 do Lote I - Serviço de Treinamento (sob demanda) (redação do art. 20, I, do Decreto 48.817/23):

a) provisoriamente, pelos fiscais dos contratos, mediante termo, no prazo de 15 (quinze) dias corridos após a entrega dos serviços, quando verificado o cumprimento das exigências de caráter técnico;

b) definitivamente, pelos fiscais ou comissão de fiscalização, após decorrido o prazo de 30 (trinta) dias corridos do recebimento provisório, mediante termo detalhado que comprove o atendimento das exigências contratuais.

28.1.4. Para o item 2 do Lote I, para o item 22 do Lote II e item 24 do Lote III - Serviço Técnico Especializado (sob demanda) (redação do art. 20, I, do Decreto 48.817/23):

a) provisoriamente, pelos fiscais dos contratos, mediante termo, no prazo de 15 (quinze) dias corridos após a entrega dos serviços, quando verificado o cumprimento das exigências de caráter técnico;

b) definitivamente, pelos fiscais ou comissão de fiscalização, após decorrido o prazo de 30 (trinta) dias corridos do recebimento provisório, mediante termo detalhado que comprove o atendimento das exigências contratuais.

28.2. O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato ou termo de referência, podendo ser fixado pelo fiscal do contrato um prazo para a substituição do bem, ou o refazimento do serviço, às custas do contratado, sem prejuízo da aplicação das penalidades, sendo sempre necessário a motivação da recusa.

28.3. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos por este Decreto e pelo contrato.

28.4. Salvo disposição em contrário constante do edital, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta do contratado.

29. CONDIÇÕES DE GARANTIA CONTRATUAL

29.1. O Contrato conta com garantia de execução, nos moldes do artigo 96 da Lei nº 14.133/2021, correspondente a 3% (três por cento) da seguinte forma:

29.2. Para os item 1 do Lote 1, itens 4, 9, 10, 13, 14, 15, 16, 17, 18, 19, 20 e 21 do Lote II, por se tratar de aquisição, a base de cálculo da garantia será o valor total do Contrato.

29.3. Para o item 2 e 3 do lote 1, item 22 do Lote II e item 24 do Lote III, por se tratar de serviço por demanda, a base de cálculo da garantia será o valor inicial atualizado do Contrato.

29.4. Para os itens 5, 6, 7, 8, 11, 12, do Lote II e item 23 do Lote III, por se tratar de serviço contínuo, a base de cálculo da garantia será o o valor anual do Contrato

29.5. O referido percentual, resguardada a discricionariedade prevista no acima citado art. 96, caput e o teto estabelecido no caput do art. 98 do mesmo diploma legal, considera a natureza do objeto (bens e serviços), enquanto ferramenta estratégica de caráter tecnológico de relevância para as atividades do órgão contratante em razão do volume de recursos financeiros envolvidos no certame, visando impedir a inexecução, mesmo que parcial do objeto e danos ao erário.

29.6. Caso o prazo de vigência do contrato seja inferior a um ano, a garantia aqui prevista será calculada sobre o valor total do Contrato.

29.7. O CONTRATADO poderá optar pelas seguintes modalidades de garantia:

a) caução em dinheiro ou em títulos da dívida pública;

b) seguro-garantia; e

c) fiança bancária.

d) título de capitalização custeado por pagamento único, com resgate pelo valor total.

29.8. Qualquer que seja a modalidade escolhida pelo CONTRATADO, a garantia assegurará o pagamento de:

a) prejuízos advindos do não cumprimento do objeto do Contrato e do não adimplemento das demais obrigações neste previstas;

b) multas moratórias, compensatórias e administrativas aplicadas pela Administração ao CONTRATADO; e

c) obrigações trabalhistas e previdenciárias de qualquer natureza, assim como as obrigações de regularidade perante o FGTS, não adimplidas pelo CONTRATADO, quando couber.

29.9. A garantia, qualquer que seja a modalidade escolhida, terá validade durante a vigência do Contrato e por mais 90 (noventa) dias após o término deste prazo de vigência.

29.10. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o CONTRATADO ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

29.11. Ressalvada a hipótese de seguro-garantia, em que deverá ser observado o prazo do item 29.13, o CONTRATADO apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do CONTRATANTE, contado da assinatura do Contrato, o comprovante de prestação de garantia, na forma do item 29.8.

29.12. Caso oferecida a modalidade de seguro-garantia, sua apresentação deve ocorrer em 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato, e observar-se-ão as seguintes condições:

a) a apólice permanecerá em vigor mesmo que o CONTRATADO não pague o prêmio nas datas convencionadas;

b) a apólice deverá acompanhar as modificações referentes à vigência do Contrato principal, mediante a emissão do respectivo endosso pela seguradora;

c) será permitida a substituição da apólice na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no item 29.11; e

d) a apólice somente será aceita se contemplar todos os eventos indicados no item 29.9, observada a legislação que rege a matéria.

29.13. Em caso de oferecimento de títulos da dívida pública, estes devem ser emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

29.14. Caso a opção seja por fiança bancária, esta deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

29.15. Caso a opção seja por garantia em dinheiro, deverá ser efetuada em favor do CONTRATANTE, na conta-corrente da instituição financeira contratada pelo Estado, cujo valor será corrigido monetariamente e restituído ao CONTRATADO, na forma do item 29.24.

29.16. O CONTRATADO obriga-se a fazer a reposição, a suplementação ou a renovação da garantia, no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificado, no caso desta ser executada, total ou parcialmente, ou o Contrato for prorrogado ou tiver o seu valor alterado, assim como em qualquer outra situação que exija a manutenção da condição disposta no item 29.1 neste item.

29.17. A inobservância do prazo fixado para apresentação, reposição, suplementação ou renovação da garantia acarretará a aplicação de multa e/ou outras penalidades, na forma disposta no contrato.

29.18. O atraso superior a 25 (vinte e cinco) dias autoriza o CONTRATANTE a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, com a aplicação das sanções cabíveis.

29.19. O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

29.20. O emitente da garantia ofertada pelo CONTRATADO deverá ser notificado pelo CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

29.21. O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções ao CONTRATADO.

29.22. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

29.23. Extinguir-se-á a garantia com a restituição da apólice, carta fiança, título da dívida pública ou autorização para a liberação da caução em dinheiro, atualizada monetariamente, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que o CONTRATADO cumpriu todas as cláusulas do contrato.

29.24. A garantia somente será liberada ou restituída, após a fiel execução do Contrato ou pela sua extinção, por culpa exclusiva da Administração, ou quando assim convencionado, em se tratando de extinção consensual da contratação.

29.25. O CONTRATADO autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista no edital e no Contrato.

29.26. No caso de inexecução total ou parcial do objeto, que acarrete a rescisão do Contrato, será automaticamente devida multa compensatória no valor de 5% do valor do Contrato, visando resguardar o órgão contratante em razão do volume de recursos financeiros envolvidos no certame.

30. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA

30.1. O presente Estudo Técnico Preliminar (ETP), bem como os seus anexos, consideram a necessidade de contratação do objeto (serviços), os requisitos técnicos, legais, ambientais e os do próprio negócio, o mercado em que o objeto se encontra inserido, bem como os demais requisitos necessários para a caracterização e quantificação da demanda identificada, bem como o processo de escolha da solução que melhor se adequa ao PRODERJ nesta oportunidade. São considerados ainda os requisitos ambientais e os aspectos legais, cabendo ressaltar que os riscos envolvidos são administráveis e os custos previstos são compatíveis e se caracterizam pela economicidade.

30.2. Desta forma, entende-se ser VIÁVEL a contratação em comento, e, visando dar início à implementação do objeto aqui delineado, recomenda-se a elaboração de Termo de Referência com base no presente estudo e o encaminhamento para o setor competente para o prosseguimento do feito.

31. ANEXOS

31.1. Abaixo, estão listados os documentos anexos cujas disposições estão em plena concordância com este documento principal do qual correspondem a parte integrante e indissociável:

I - Especificações Técnicas do Objeto (128113020);

II - Catálogo de serviços (128113089);

III - Prova de Conceito I (128113468);

IV - Prova de Conceito II (128113223); e

V - Mapa de Riscos (128113966).

32. RESPONSÁVEIS

32.1. RESPONSÁVEL PELA REVISÃO

Rodolfo Targino de Araújo Assistente de Planejamento de Contratações ID 5167673-7

32.2. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Roberto Charles Vilas Diretor de Infraestrutura Tecnológica ID 4372004-8	**Luís Cláudio Marinho Coelho** Gerente de Rede e Telecomunicações ID 5140902-0	**Charles Monteiro Guimarães** Diretor de Patrimônio e Logística ID 4432892-3	**Marco Antonio de Andrade** Assessor-Chefe VPA ID 4284601-3

Rio de Janeiro, na data da assinatura eletrônica.

Documento assinado eletronicamente por **Rodolfo Targino de Araujo**, **Assistente**, em 23/03/2026, às 14:13, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Luís Cláudio Marinho Coelho**, **Gerente**, em 23/03/2026, às 14:24, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor-Chefe**, em 23/03/2026, às 14:27, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Roberto Charles Vilas**, **Diretor**, em 23/03/2026, às 14:28, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 23/03/2026, às 14:33, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **128112124** e o código CRC **5B92B5E7**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

ANEXO I

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1. INTRODUÇÃO DA ESPECIFICAÇÃO DETALHADA DO OBJETO

- **LOTE I**
- **ITEM 1: SOLUÇÃO DE MONITORAMENTO DE COMPORTAMENTO ANÔMALO DA REDE, DETECÇÃO, ANÁLISE E RESPOSTA DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO, COM INSTALAÇÃO DA SOLUÇÃO.**

1.1. Requisitos Mínimos Gerais

1.1.1. A solução de segurança deverá ser composta de dispositivo do TIPO Appliance Físico mais softwares necessários. Poderá ser composta por um ou mais softwares licenciados para atender ao requisitado. Deve ser entregue plenamente interoperáveis entre si e ser do mesmo fabricante.

1.1.2. "A solução a ser contratada, possui métrica de consumo por Gbps. Para cada Gbps de performance contratado, a CONTRATADA deverá entregar as funcionalidades aqui exigidas, definindo da melhor forma, quais equipamentos físicos e soluções virtuais devem ser ofertadas para atender ao requisito da CONTRATANTE. Caso a solução demande de quantidade de dispositivos e/ou IPs para precificação, deve ser considerado 1.300 (mil e trezentos) dispositivos por cada Gbps de proteção entregue;

1.1.3. Cada Gbps contratado deverá contar com as especificações aqui citadas. Para que tornem- se viáveis e simplificadas as aquisições de cada Gbps de deteção e resposta, as contratações desta solução completa devem ser consideradas em pacotes mínimos de 2Gbps, 5Gbps ou 10Gbps, além de combinações desses valores;

1.1.4. As funcionalidades de detecção (sensor de detecção), deverão ser obrigatoriamente entregues em formato de Appliance física. As demais funcionalidades podem opcionalmente, serem fornecidas como Appliance virtual;

1.1.5. Todos os módulos e componentes que compõem a solução deverão se integrar, visando a homogeneidade do ambiente tecnológico para análise de tráfego, monitoramento, investigação, defesa, prevenção e resposta a ameaças e incidentes;

1.1.6. Toda a solução deve ser compatível com os componentes lógicos e físicos em operação no ambiente do CONTRATANTE, tais como servidores, AD (Active Directory), IPS, SIEM, WAF, switches de rede, firewall, etc, funcionando sem impacto à essas soluções;

1.1.7. A solução deverá permitir a detecção avançada de ameaças baseada em comportamento com analise de incidentes baseado em IA ou execução de machine learning no core central da solução sem necessidade de analise ou consulta de base de dados externas;

1.1.8. A retenção, por parte da solução, dos fluxos de rede (network flows) e seus respectivos metadados, bem como incidentes, eventos e demais informações, deve ser por um período mínimo de 90 (noventa) dias corridos;

1.1.9. A solução deverá possuir ferramenta do tipo honeypot (sistema configurado como uma espécie de emboscada mediante a emulação de um alvo para atrair ataques cibernéticos, registrando as tentativas de intrusão para obter informações e o comportamento dos cyber-criminosos. A solução deverá permitir a detecção avançada de ameaças baseada em comportamento.

1.1.10. A solução deverá prover os seguintes perfis de acesso, a fim de permitir a visualização de incidentes/eventos em tempo real, alertas, status das ações tomadas, etc:

1.1.10.1. Alta administração (coordenadores, gestores);

1.1.10.2. Equipe técnica (painel completo e detalhado);

1.1.10.3. Auditores (auditor interno, auditores externos etc.).

1.2. Requisitos de Arquitetura Tecnológica

1.2.1. Toda a solução (hardware e software) fornecida deverá ser de um único fabricante em que seus módulos e/ou programas sejam totalmente integrados, de modo a preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes e a facilidade de uso e operação;

1.2.2. A solução deverá vir acompanhada de todos os elementos/acessórios necessários à sua implantação (conectores, cabeamentos, etc.);

1.2.3. Nenhum dos componentes da solução poderá ter seu end-of-sale e end- of-life anunciado no momento do aceite definitivo de sua entrega. Caso seja essa a situação, o fornecedor deverá entregar um modelo equivalente ou superior ao que entrou nas situações anteriores;

1.2.4. No caso do anúncio end-of-sale e end-of-life ocorrer após o aceite definitivo da entrega da solução, o end-of-support não poderá ocorrer nos próximos 30 (trinta) meses, a contar da emissão do anúncio;

1.2.5. Todos os componentes da solução (hardwares e softwares) deverão ser fornecidos com todas as licenças necessárias ao seu pleno funcionamento, de modo a realizar todas as funcionalidades requeridas;

1.2.6. Não serão aceitas soluções com software e hardware de fabricantes distintos, ou mesmo soluções de uso geral como Servidores, Estações de Trabalho ou Equipamentos como Blades.

1.2.7. As licenças a que se refere o item anterior deverão ter caráter perpétuo, não precisando de renovação, de modo que, após o tempo de contrato, a solução permaneça indefinidamente plenamente funcional, devendo sua atualização (subscrição) ser garantida pelo prazo do contrato;

1.2.8. Os equipamentos devem possuir profundidade dentro dos padrões;

1.2.9. dos racks; caso não se enquadrem neste padrão, deverá ser fornecido todos os requisitos para a fixação no rack (bandeja, parafuso, etc);

1.2.10. Todos os equipamentos devem ser fornecidos com cabos de energia com no mínimo 1,80m já com o plug no padrão hoje utilizado pelo CONTRATANTE, cabendo ao Licitante durante a oportunidade de vistoria verificar o modelo (ou solicitar a informação via e-mail ou contato telefônico), para que o fornecimento ocorra de acordo com a necessidade do CONTRATANTE. Caso não seja do mesmo padrão, deverá ser considerado o fornecimento de adaptadores para o citado padrão;

1.2.11. A solução deve permitir a possibilidade de deploy em Cluster de Alta disponibilidade (HA).

1.3. **Requisitos Mínimos do Appliance para análise de comportamento anômalo da rede (sensor)**

1.3.1. O(s) appliance(s) e o(s) sistema(s) proposto(s) devem atender às características técnicas mínimas obrigatórias exigidas em cada item;

1.3.2. Deve ser novo e de primeiro uso, devendo estar em linha de produção, com a última versão de software e/ou firmware disponível e sendo comercializado pelo Fabricante;

1.3.3. Suportar arquitetura MASTER-SLA VE, onde a análise e correlação de dados são locais, e apenas metadados são encaminhados para o MASTER (administração centralizada);

1.3.4. Cada appliance entregue para suportar o throughput solicitado deve possuir altura de, no máximo, 1U, para ser instalado em rack de 19” e ser fornecido com o kit de instalação;

1.3.5. Cada Gbps contratado deve possuir pelo menos 200GB SSD de espaço de armazenamento, podendo o total ser compartilhado entre os Gbps contratados;

1.3.6. Deve suportar 500 mil sessões simultâneas;

1.3.7. Deve suportar 30 mil novas sessões/segundos com tráfego HTTP;

1.3.8. Caso a solução possua métrica de dispositivos e/ou IPs gerenciados, deverá ser considerado 1.300 (mil e trezentos) dispositivos/IP por Gbps entregue;

1.3.9. O(s) appliance(s) entregue(s) para suportar o throughput solicitado devem possuir capacidade de processamento e memória suficiente para operar com todas as funcionalidades contratadas simultaneamente e no volume máximo de tráfego estabelecido;

1.3.10. Cada appliance entregue para suportar o throughput solicitado devem possuir 2 (duas) fontes de alimentação redundante, do tipo hot-swappable, com alimentação de 100~120VAC e 210~240VAC e frequência de 50 ou 60 Hz ou auto-ranging;

1.3.11. Cada Gbps contratado deverá possuir, em sua appliance física, no mínimo, 2 (duas) interfaces de 10 Gbps (SFP+), 1 (uma) interfaces de 1Gbps (SFP) ou 1 (uma) interfaces GE, para ligação física ao switch core do ambiente local, devendo estar acompanhado de seus respectivos transceivers para realizar essa conexão;

1.3.12. A plataforma deve ser capaz de monitorar todo o comportamento do tráfego da rede interna do CONTRATANTE, a partir da captura de pacotes espelhados para a appliance através do switch core local;

1.3.13. A solução deve ser capaz de monitorar o tráfego em pacotes Jumbo Frame.

1.4. **Requisitos de Detecção de Incidentes (Incident Detection)**

1.4.1. A solução deve criar linhas de base dos logs dos ativos de sustentação, visando montar um perfil do risco e do consumo de cada um deles;

1.4.2. A solução deve executar o correlacionamento dos eventos para detectar táticas, técnicas e procedimentos de ataques, identificados pela modelagem de ameaças desenvolvida pelo MITRE, disponível em https://attack.mitre.org/;

1.4.3. A solução deve detectar ataques internos (leste-oeste) e externos (norte- sul) contra a infraestrutura de TIC do CONTRATANTE;

1.4.4. A solução deve identificar os seguintes casos de uso nos ativos de sustentação:

1.4.4.1. Execução de programas maliciosos (exploits ou payloads);

1.4.4.2. Movimentação lateral;

1.4.4.3. Escalação de privilégios;

1.4.4.4. Sinalização (beaconing) ou conexão com Centrais de Comando e Controle;

1.4.4.5. Exfiltração de dados;

1.4.4.6. Ataques fileless, via Powershell;

1.4.4.7. Exploração de vulnerabilidades dos ativos de sustentação, de conhecimento público, publicada pelo MITRE em https://cve.mitre.org/;

1.4.4.8. Varreduras de portas tcp e udp;

1.4.4.9. Tráfego de IPs inscritos em listas negras, públicas ou privadas;

1.4.4.10. Tentativas de login em horário atípico;

1.4.4.11. Quebra de senha;

1.4.4.12. Surto de worm / vírus.

1.4.5. A solução deverá identificar no mínimo os seguintes casos de uso de detecção em aplicações web:

1.4.5.1. Ataques de Injeção SQL;

1.4.5.2. Ataques de Cross site scripting;

1.4.5.3. Todos os ataques da Web de camada 7 via internet / intranet;

1.4.5.4. Tentativa de violação de acesso.

1.4.6. A solução deverá identificar ataques a partir do tráfego da rede, incluindo, mas não se limitando a:

1.4.6.1. Movimentação lateral;

1.4.6.2. Beacon de malware;

1.4.6.3. Exfiltração de dados;

1.4.6.4. Ransomware.

1.4.7. Além dos casos de uso detecção de uso definidos estaticamente, a solução deverá incorporar Inteligência Artificial (IA) e/ou Machine Learning (ML) para detectar anomalias, a fim de acelerar a análise de comportamento incomum nos ativos de sustentação;

1.4.8. A solução não deve se basear apenas em assinaturas estáticas do tipo IPS/IDS, mas sim também suportar assinaturas personalizadas, atualizações manuais de inserção ou extração de assinaturas automáticas e uma enciclopédia de ameaças incorporada;

1.4.9. A solução deve suportar detecção e proteção de anomalias de protocolo, incluindo os protocolos SMTP, IMAP, POP3, VOIP e HTTP;

1.4.10. A solução deve ter a função de captura de pacotes;

1.4.11. A solução deve ser compatível com o Flow Based Antivirus para os protocolos SMTP, POP3, IMAP, FTP e HTTP;

1.4.12. A solução deve suportar a detecção de vírus para arquivos;

1.4.13. Compactados como RAR, ZIP e TAR;

1.4.14. A solução deve ser capaz de analisar novos ataques de maneira autonoma baseado em IA sem uso de assinaturas ja conhecidas;

1.4.15. A solução deve suportar a descoberta eficaz de bots de intranet e a prevenção de novos ataques avançados de ameaças, comparando as informações obtidas com o banco de dados de endereços de C&C;

1.4.16. A solução deve suportar atualização automática da biblioteca local de assinatura de defesa contra Botnet/C&C;

1.4.17. A solução deve suportar a detecção do DoS/DDoS e SYN Flood;

1.4.18. A solução deve possuir ambiente de execução virtual de malware (sandbox), baseado em nuvem para encontrar ameaças desconhecidas;

1.4.19. A solução deve suportar o upload de arquivos maliciosos para sandbox na nuvem para análise;

1.4.20. A solução deve suportar o upload de arquivos maliciosos de protocolos incluindo SMTP, FTP, HTTP/HTTPS, IMAP e POP3;

1.4.21. A solução deve suportar o compartilhamento global de inteligência de ameaças, para detectar a nova ameaça desconhecida;

1.4.22. A solução deve suportar classificação e detecção de spam em tempo real. A solução deve suportar as categorias de Spam Confirmado, Spam Massivo e Spam Suspeito;

1.4.23. A solução deve suportar a detecção, independentemente do idioma, formato ou conteúdo da mensagem;

1.4.24. A solução deve suportar os protocolos de e-mail SMTP e POP3;

1.4.25. A solução deve suportar lista de permissão para e-mails de domínios confiáveis;

1.4.26. Identificação de envio/recebimento para contas pessoais externas através de políticas configuradas.

1.5. **Requisitos para Análise de Incidentes (Incident Analysis)**

1.5.1. A solução deverá possuir capacidade de busca de todas as sub-redes no ambiente e quantidade de dispositivos através de maneira ativa via scan sobre a rede e de maneira passiva, através de identificação de tráfego observado;

1.5.2. A solução deverá suportar algoritmos de triagem orientados por máquina (Machine Learning), que considere parâmetros contextuais, comportamento histórico e inteligência de ameaças externas, a fim de definir a severidade/pontuação para o incidente, em tempo real. A referida severidade/pontuação deve servir de base para priorizar alertas e outras ações referentes ao incidente:

1.5.3. O feed de inteligência de ameaças também deve ser utilizado para identificar ataques por meio de agentes mal-intencionados;

1.5.4. A solução deverá oferecer suporte a um mecanismo que permita a adequação das regras;

1.5.5. A solução deverá permitir a investigação de alertas de triagem personalizados considerada crítica;

1.5.6. A solução deverá oferecer suporte à pesquisa rápida em conjuntos de dados gerados, com base em critérios personalizados ou exportação dos dados para solução de SIEM;

1.5.7. A solução deverá possuir recursos para analisar o impacto do ataque no ativo alvo, incluindo indicadores de comprometimento (IOCs), conexões de rede externas;

1.5.8. A solução deverá oferecer suporte para analisar e identificar o impacto de um ataque nos ativos de sustentação;

1.5.9. A solução deverá fornecer recursos de gerenciamento para armazenar evidências relativas a um alerta específico ou conjunto de alertas;

1.5.10. A solução deverá oferecer suporte à pesquisa rápida em conjuntos de dados armazenados, com base em critérios personalizados;

1.5.11. A solução deverá fornecer recursos para fazer análise visual do fluxo de alertas, integrada ao log de evidências, objetivando proporcionar uma análise eficiente, com opções para rastrear a cadeia de ataque em qualquer escala;

1.5.12. A solução deverá ser capaz de definir, desenvolver e implementar casos de uso de detecção dos incidentes, observada a modelagem de ameaças previstas no framework ATT&CK, a fim de avaliar o tratamento de todas as etapas do ciclo de vida do ataque.

1.6. **Requisitos de Resposta a Incidentes (Incident Response)**

1.6.1. A solução deve elaborar e programar fluxos de trabalho (playbooks) capazes de orquestrar e automatizar as atividades de resposta a incidentes, inclusive com tratamento de falso positivo, listas brancas, escalonamento e indicadores para gestão;

1.6.2. O sistema deverá analisar um incidente a partir de uma base de dados analítica de evidências e indícios de ataques;

1.6.3. O sistema deverá manter o controle da primeira resposta e das medidas subsequentes tomadas no incidente;

1.6.4. O sistema deverá registrar a ordem cronológica dos eventos;

1.6.5. O sistema deverá registrar os IOCs e artefatos relacionados ao incidente;

1.6.6. A plataforma deverá permitir, em conjunto com a equipe de segurança do CONTRATANTE, a forma de registro de comentários e orientações, preservação do histórico de conversa, e capacidade de adicionar artefatos e evidências;

1.6.7. A resposta adequada e automatizada será utilizada para executar roteiros pré-aprovados juntamente com a equipe de segurança do CONTRATANTE, e ter a capacidade de se integrar tais como: bloquear IP¿s no firewall e criação de políticas de segurança;

1.6.8. Espera-se não apenas uma solução que tenha capacidade de integração com outras soluções existentes para resposta aos incidentes, mas também que a própria solução (através de componente nativo ou componente adicional) execute a remediação. A contratada se torna responsável pela entrega da solução completa que será inserida à rede da Contratante para bloqueio em tempo-real ou próximo à tempo-real, das ameaças identificadas pela solução;

1.6.9. A solução deverá ter capacidade de remediar e prevenir ameaças encontradas de acordo com os padrões citados anteriormente, possuindo assim capacidade de prevenção contra intrusões (IPS);

1.6.10. Essas prevenções devem ocorrer a nível de rede, e não serão permitas soluções que dependam da solução de firewall em uso, ou de outro componente da estrutura do Contratante. Devendo a solução ser entregue de forma completa a fim de identificar, correlacionar, analisar, e responder às ameaças de forma autônoma;

1.6.11. A solução deve permitir que se crie listas de permissão (whitelists) para o módulo de remediação;

1.6.12. Deverá ser entregue solução dedicada para prevenção e bloqueio (Sistema de Prevenção - IPS), que deverá ser do mesmo fabricante das demais soluções ofertadas além de, obrigatoriamente, ser entregue em formato de hardware, com capacidade de throughput equivalente à 1Gbps de throughput de IPS para cada 1Gbps de detecção entregue. Deve ainda oferecer para cada Gbps entregue, minimamente, 2 (duas) interfaces, sendo 1 (uma) de GE e 1 (uma) 1Gbps no padrão SFP, com seus respectivos transceivers instalados;

1.6.13. A remediação através de função de prevenção, deve suportar as seguintes ações:

1.6.13.1. Monitorar;

1.6.13.2. Bloquear;

1.6.13.3. Reset (IP do atacante, IP da vítima ou interface de entrada), com tempo de expiração.

1.6.14. A solução deverá fornecer relatórios de respostas aos incidentes;

1.6.15. A solução deve permitir visualização gráfica de, onde as informações apresentadas devem ser por ativos afetados, total de ativos, ativos por classificação de risco, sumário das violações por fase do ataque, sumário dos por tipo;

1.6.16. A solução deverá identificar o tráfego de rede atípico promovido por aplicativos, como por exemplo compartilhamento de arquivos, comunicação peer-to-peer (P2P), dentre outros;

1.6.17. A solução deverá produzir informações por meio da investigação de ataques, devendo estar estruturadas para apoiar o serviço de detecção;

1.6.18. A solução deve ser capaz de realizar a mitigação de maneira nativa nos principais NGFW listados no Gartner;

1.6.19. A solução deve permitir a criação de Templates customizados para aplicar a mitigação via SSH.

1.7. **Requisitos para Investigação de Ameaças (Cyber Threat Hunting)**

1.7.1. A plataforma deve utilizar algoritmos e ferramentas para investigar ativa e proativamente ataques que estejam sendo perpetrados na infraestrutura de TI, e encaminhar alertas a serem analisados pelos analistas de detecção;

1.7.2. A plataforma deve ser capaz de estabelecer, desenvolver, programar, atualizar e manter uma estrutura de investigação que contemple:

1.7.3. Ações que identifiquem atividades maliciosas que ainda não tenham gerado alertas;

1.7.4. Ações apoiadas por indicadores de comprometimento (IOC), recebidos de centrais de Cyber Threat Intelligence;

1.7.5. A solução deverá possuir capacidade manter base de conhecimento de IOCs e possuir integração com soluções de Threat Intel;

1.7.6. A solução deverá possuir capacidade de detectar ataques desconhecidos;

1.7.7. A solução deverá possuir modelos aptos a detectar estágios de uma cadeia de ataque cibernético;

1.7.8. A solução deverá elencar os casos de uso que podem detectar ataques, usando técnicas de aprendizado de máquina e modelos analíticos;

1.7.9. A solução deverá possuir modelos de Inteligência Artificial (IA) com Machine Learning embarcada, sem conectividade externa, para detectar ataques desconhecidos de agentes desconhecidos;

1.7.10. A solução deverá possuir modelos analíticos para detectar diferentes estágios de cadeia de ataques.

1.8. **Requisitos para Inteligência de Ameaças e Automação Central**

1.8.1. A solução deverá possuir console baseada em software, que permita a centralização dos eventos e a resposta de bloqueio às ameaças. Essa console central deve estar preparada para o eventual crescimento da quantidade de sensores de detecção de ameaças no ambiente no CONTRATANTE;

1.8.2. Para total atendimento as especificações solicitadas, pode-se realizar composição com solução adicional, desde que não seja software livre. Caso a solução adicional não seja do mesmo fabricante da solução principal, deve possuir integração nativa entre as plataformas, e com ponto único de suporte;

1.8.3. A console central poderá ser embarcada dentro dos sensores NDR ou separadamente. No caso de versão apartada, deverá ser virtual e instalada em localmente no ambiente da CONTRATANTE, devendo estar disponível de forma local (on-site), em modelo virtual. Deve estar disponível para instalação em ambientes virtuais VMware ESXi e Hyper-V;

1.8.4. A solução deverá fornecer painel central para demonstrar o risco da organização para tratar as ameaças;

1.8.5. A solução deverá fornecer painel de segurança abrangente, baseado na web, para visualização de incidentes/eventos em tempo real, alertas, status das ações tomadas, indicadores do ranking das ameaças, dentre outros;

1.8.6. Para a console de centralização dos eventos e ameças ou para o próprio sensor NDR, caso possua métrica ou limitação de EPS (Eventos por segundo), a solução deve ser capaz de tratar até 1.500 (mil e quinhentos) EPS para coleta por Gbps entregue, para processamento, armazenamento e corelacionamento dos eventos de rede, de forma sustentada. Caso a solução possua métrica de dispositivos e/ou IPs, deverá ser considerado 1.300 (mil e trezentos) dispositivos/IP por Gbps entregue;

1.8.7. A solução deverá oferecer resposta automatizada para incidentes, por meio da conexão remota a outros componentes através de SSH, HTTP ou API com IPS, WAF, switches de rede, firewalls e roteadores;

1.8.8. A solução deve ser capaz de coletar eventos de todos os ativos de sustentação do ambiente, e normalizá-los em um formato padrão para possibilitar a sua estruturação, correlação, criação de regras de análises e resposta a incidentes;

1.8.9. A solução deverá se integrar com as fontes de log de segurança (como SIEM, EDR, EPP, IAM, PAM e outros), via protocolo Syslog, a fim de ingerir dados do ambiente e enriquecer as investigações de ameaças;

1.8.10. A solução deverá suportar Netflow para recebimento de flows de rede a fim de ingerir dados do ambiente e enriquecer as investigações de ameaças;

1.8.11. Deve possuir banco de dados de inteligência de domínios DNS, códigos maliciosos, IP, vulnerabilidades, detecções de intrusão e geolocalização;

1.8.12. Deve suportar análise de killchain e integração com o MITRE ATT&CK para definição de técnica e tática;

1.8.13. Deve suportar pesquisa por palavras-chave, termos e filtros baseados em SPL, Elastic ou similar;

1.8.14. A solução deve suportar REST API;

1.8.15. Deverá possuir capacidade de criação de regras para automação de respostas através de fluxos de trabalho (playbooks), com regras pré-definidos e capacidade de criação de regras customizados através da interface gráfica;

1.8.15.1. A funcionalidade de automação de respostas, deverá ainda permitir que estas regras sejam utilizados para automação de respostas aos incidentes conforme configuração de gatilhos (triggers);

1.8.15.2. Essas triggers a serem usadas, podem ser eventos/características de ameaças, consulta de inteligência de ameaças, condições de julgamento para resposta automática e ações de processamento de resposta (políticas de emissão, bloqueio de IP ou criação de ordens de serviço), de modo a realizar resposta automática diretamente pela solução contratada ou através de outro dispositivo;

1.8.15.3. Caso a solução não possua funcionalidade nativa de respostas através de fluxos de automação, poderá ser entregue solução adicional, desde que possua integração com a ferramenta de deteção e respostas ofertada, que não seja software livre e que ainda possua licenciamento adequado para 10 usuários e/ou 1.500 EPS por Gbps de deteção entregue;

1.8.16. Deve suportar a geração de relatórios de ameaças e eventos;

1.8.17. A solução deverá ser capaz de tomada de decisões por meio validação em fontes externas, tornando mais eficiente o processo de identificação, reduzindo deste modo os falsos positivos;

1.8.18. A solução deverá fornecer inteligência de nível estratégico contra ameaças, por meio de notificações de incidentes e violações que ocorrem na web, permitindo identificar:

1.8.18.1. Quais são os IoC's relacionados às ameaças;

1.8.18.2. Quais etapas de mitigação devem ser tomadas para conter a ameaça.

1.8.19. A plataforma central de inteligência de ameaças deve receber dados de todos os ativos de sustentação, tráfegos de rede, eventos de segurança e usuários, de modo a fornecer informações sobre impacto de ameaças sobre os ativos do CONTRATANTE, e destacar os riscos identificados, e sugestões de remediação.A solução deverá possuir algoritmos para avaliar automaticamente um ativo, e atribuir um valor de risco ao mesmo;

1.8.20. A solução deverá oferecer suporte à integração usando STIX ou TAXII para ingestão de informações de ameaças ou endereços maliciosos;

1.8.21. A solução deverá oferecer integração com soluções de terceiros via API configurável;

1.8.22. A solução deve apresentar visão agregada de todos os sensores que houver na rede, em um único local, e com visão no mínimo para:

1.8.22.1. Agregação de lista de eventos por endereço do atacante;

1.8.22.2. Agregação de lista de eventos por endereço da vítima.

1.9. **SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO E IMPLEMENTAÇÃO**

1.9.1. Para todos os produtos da solução (hardware ou software) adquirida, a Contratada deverá fornecer serviço especializado de instalação, configuração e implementação da solução no ambiente do CONTRATANTE.

1.9.2. A Contratada deverá realizar o armazenamento, a embalagem e desembalagem, o transporte, a entrega e a instalação de todo e qualquer item da solução no local de implantação da solução.

1.9.3. Os serviços especializados de instalação, configuração e implementação deverão ocorrer em dias úteis, no horário compreendido entre 8:00h e 17:00h, salvo definição contrária estabelecida em comum acordo entre Contratante e Contratada.

1.9.4. O serviço de instalação, configuração e implementação deverá ser agendado previamente com a equipe técnica do CONTRATANTE.

1.9.5. Entende-se por serviço instalação, configuração e implementação a montagem física de todos os equipamentos da solução adquirida (incluindo o fornecimento, por parte da Contratada, de trilhos de fixação e cabos UTP ou FO), a configuração e interligação física (cabeamento) e lógica à rede de dados do CONTRATANTE, bem como a instalação e configuração dos softwares necessários ao pleno funcionamento da solução, sendo a Contratada responsável integral por todo o escopo referente a este item.

1.9.6. Os serviços especializados de instalação, configuração e implementação deverão ser executados por profissionais alocados pela Contratada, que deverão ser devidamente certificados pelos respectivos fabricantes dos produtos ofertados, sendo que tal condição deverá ser demonstrada mediante documento de comprovação (certificação técnica na plataforma a ser implantada) durante a execução do objeto.

1.9.7. As despesas de viagens, hospedagem, diárias, alimentação e demais para execução dos serviços correrão integralmente por conta da Contratada.

1.9.8. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, podendo estas ser realizadas presencialmente ou via conferência web, devendo a futura Contratada sugerir as configurações de acordo com normas e boas práticas, cabendo ao CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas.

1.9.9. A Contratada deverá agendar visitas técnicas de pré-instalação (site survey) nas dependências designadas pelo CONTRATANTE para definição do posicionamento dos equipamentos, da instalação elétrica e demais requisitos necessários à instalação física da solução. As visitas deverão ser realizadas em até 5 (cinco) dias corridos contados da assinatura do Contrato, e o produto destas visitas técnicas será um relatório detalhado do site survey, a ser elaborado pela Contratada, e posteriormente apresentado na reunião de abertura de projeto (kick-off).

1.9.10. A Contratada deverá fazer análise do ambiente tecnológico atual, devendo o CONTRATANTE fornecer:

1.9.10.1. Informações necessárias sobre a infraestrutura instalada, de modo que se possa assegurar a continuidade dos serviços prestados pelo CONTRATANTE durante a migração, mantendo a disponibilidade dos serviços básicos de rede (resolução de nomes, endereçamento dinâmico, autenticação dos usuários, etc.), e dos demais serviços de retaguarda (aplicativos, correio eletrônico, banco de dados, Internet, etc.);e

1.9.10.2. Informações necessárias à implantação da solução, como topologia de rede, VLANs, endereçamento IP, portas de switches que devem ser utilizadas e outras necessárias à perfeita configuração e interligação.

1.9.11. A Contratada deverá apresentar um Projeto Executivo, que será avaliado e aprovado pela equipe técnica do CONTRATANTE, contendo no mínimo o seguinte:

a) descrição dos equipamentos e softwares que deverão ser instalados;

b) deverão ser descritos pré-requisitos com os recursos e condições que deverão ser providos pelo CONTRATANTE, necessários para que a Contratada possa realizar os serviços de instalação;

c) relatórios das visitas técnicas (site survey) de pré-instalação;

d) atividades a serem desenvolvidas, incluindo cronogramas;

e) desenho da arquitetura lógica da solução, contendo a topologia da solução, indicando as alterações com relação à topologia atual;

f) desenho da arquitetura física da solução, contendo tabela de conectividade física da solução, com o mapeamento das conexões necessárias diretamente nos dispositivos de rede do CONTRATANTE;

g) políticas de configuração dos elementos da solução;

h) ações de rollback, descrevendo as ações necessárias para restabelecimento do ambiente à normalidade, no evento de falhas no funcionamento das novas soluções que causem interrupção no fluxo de dados da rede;

i) Caderno de Testes e Homologação, para validação da solução.

1.9.12. O CONTRATANTE será responsável pelo fornecimento de listagem com todas as aplicações/sistemas que serão configuradas na implantação.

1.9.13. No prazo de até 5 (cinco) dias corridos, a partir do recebimento formal do Projeto Executivo, o CONTRATANTE deverá se manifestar sobre sua aprovação. Caso seja(m) necessário(s) ajuste(s) no documento, este será devolvido à Contratada e será concedido à mesma um novo prazo de até 2 (dois) dias corridos, para elaboração e entrega da versão definitiva do citado documento, a ser aprovada pelo CONTRATANTE.

1.9.14. Será de total responsabilidade da Contratada o dimensionamento da solução a ser implantada na rede do CONTRATANTE, sendo este sujeito à análise e validação da equipe técnica do CONTRATANTE, em conformidade aos requisitos solicitados na contratação.

1.9.15. Caso o dimensionamento feito pela Contratada não apresente desempenho satisfatório, baseado nas recomendações do fabricante e conforme exposto no item anterior, a solução deverá ser redimensionada sem ônus adicional para o CONTRATANTE, mesmo que o redimensionamento envolva adição/substituição de hardware e software.

1.9.16. Os serviços especializados de instalação, configuração e implementação deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante, em seus manuais de instalação e configuração e/ou em artigos técnicos.

1.9.17. A equipe técnica do CONTRATANTE acompanhará e supervisionará todas as etapas de instalação física dos equipamentos no Datacenter.

1.9.18. A solução apresentada não pode causar impacto na operação da rede do PRDERJ (por exemplo, lentidão na rede local, degradação no desempenho dos ativos, entre outros).

1.9.19. A implementação da solução deve ser planejada e executada de modo que não cause interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional do CONTRATANTE; caso não seja possível manter a disponibilidade dos serviços básicos no momento da instalação, as manobras de implantação deverão ser executadas durante janela de manutenção agendada previamente, em horários que não comprometam o funcionamento das atividades do órgão, inclusive aos sábados, domingos e feriados, sem ônus adicional para o CONTRATANTE.

1.9.20. O Caderno de Testes e Homologação consiste num documento onde estão descritos todos os testes a serem realizados a fim de verificar todas as funcionalidades dos produtos oferecidos e os resultados aguardados para cada teste executado, bem como avaliar o perfeito funcionamento dos produtos, em conformidade às especificações definidas quando da contratação do objeto e à proposta da Contratada, e a sua compatibilidade com a estrutura já existente no CONTRATANTE.

1.9.20.1. Os testes serão realizados pela Contratada após a instalação e configuração dos produtos, e deverão ser acompanhados pela equipe técnica do CONTRATANTE.

1.9.20.2. Caso seja detectado qualquer problema nos testes, em qualquer funcionalidade, a Contratada deverá efetuar as devidas correções e, após a realização dessas, os testes serão reiniciados.

1.9.20.3. Caso todos os testes executados logrem êxito, os produtos serão considerados implantados.

1.9.20.4. A homologação somente poderá ser iniciada após a conclusão da implantação.

1.9.20.5. Pelo menos um técnico da Contratada deverá acompanhar presencialmente o decorrer dos procedimentos de homologação.

1.9.20.6. No decorrer dos procedimentos de homologação, não deve ocorrer qualquer falha ou interrupção em qualquer uma das funcionalidades dos produtos fornecidos.

1.9.21. Em caso de qualquer falha ou interrupção em qualquer uma das funcionalidades, a Contratada deverá efetuar as devidas correções e, após a realização destas correções, a homologação será reiniciada.

1.9.22. Na ausência de qualquer falha ou interrupção em qualquer uma das funcionalidades, a solução será considerada homologada.

1.9.23. Caso seja constatada a ocorrência de divergências na especificação técnica ou qualquer outro defeito de operação durante quaisquer etapas da instalação da solução, fica a Contratada obrigada a providenciar a sua correção ou a substituição dos produtos adquiridos.

1.9.24. Em caso de detecção de anormalidades ou problemas, o CONTRATANTE comunicará formalmente os problemas detectados e a inconclusão da instalação, sendo que a Contratada terá prazo adicional de 10 (dez) dias úteis, contados a partir do dia seguinte à confirmação de recebimento da comunicação, para sanar os problemas/anormalidades detectados, sujeitando-se a Contratada às sanções e/ou penalidades previstas.

1.9.25. Para todos os efeitos, a conclusão dos serviços de instalação, configuração e implementação será atestada pela entrega da solução em pleno funcionamento, incluindo documentação técnica (as-built) contendo planejamento, relatório de todos os procedimentos realizados, parametrizações, testes realizados e seus resultados, de acordo com as especificações do(s)fabricante(s) e demais condições estabelecidas contratualmente.

1.9.26. Os serviços de fornecimento do objeto, isto é, a execução completa dos serviços e tarefas previstas por todas as etapas de trabalho conforme o Cronograma de Execução, deverão ser executados no prazo máximo de até 120 (cento e vinte) dias consecutivos a partir da assinatura da Ordem de Fornecimento de Bens.

1.9.27. Caberá à Contratada o irrestrito cumprimento de, no mínimo, as seguintes prerrogativas:

1.9.27.1. Realizar a transferência de conexão dos equipamentos conectados à rede LAN existente no CONTRATANTE para todos os equipamentos da solução adquirida;

1.9.27.2. Adequar e configurar os produtos fornecidos ao longo das etapas destinadas a colocar a solução em produção;

1.9.27.3. Executar a integração de todos os produtos da solução, de modo a não prejudicar as atividades mantidas nos locais, podendo ser exigida a realização de algumas fases em horários noturnos e fins de semana para que seja cumprido o cronograma;

1.9.27.4. Providenciar o planejamento de testes, fornecendo um “Plano de Homologação e Testes” contendo todo o processo de homologação dos produtos e detalhamento dos testes que serão executados para validar a solução implementada;

1.9.27.5. Realizar uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente, seguindo os procedimentos definidos no “Plano de Homologação e Testes”, sendo tais testes a serem obrigatoriamente executados nos componentes de hardware e software envolvidos no projeto;

1.9.27.6. Elaborar a “Documentação e Finalização do Projeto”, que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e ou gerencial.

1.9.28. Os serviços especializados de instalação e implementação deverão ser executados por profissionais alocados pela Contratada, que deverão ser devidamente certificados pelos respectivos fabricantes dos produtos ofertados, sendo que tal condição deverá ser demonstrada mediante documento de comprovação (certificação técnica na plataforma a ser implantada) durante a execução do objeto.

- **ITEM 3: Treinamento**
- **ITEM 2: SERVIÇO TÉCNICO ESPECIALIZADO DE MONITORAMENTO DE COMPORTAMENTO ANÔMALO DA REDE, DETECÇÃO, ANÁLISE E RESPOSTA DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.**

1.9.29. Os **Serviços Técnicos Especializados** Serão utilizados na operacionalização da solução, com apoio presencial de pessoal especializado ou remoto caso definido pela contratante, devendo ser solicitado mediante emissão de ordem de serviço, informando as aplicações que farão parte do escopo do serviço.

1.9.30. Todas as atividades desempenhadas relativas aos **Serviços Técnicos Especializados** deverão ser executadas nas dependências da contratante ou de maneira remota caso definido pela contratante, respeitando o horário de funcionamento da mesma, e com o acompanhamento e ciência dos servidores.

1.9.31. Demais detalhamento do serviços Técnicos Especializados estão definidas no ANEXO II do Catálogo de Serviço.

- **ITEM 3: Treinamento da Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.**

1.9.32. Visando capacitar a equipe técnica do CONTRATANTE na operacionalização plena da solução completa, a Contratada deverá executar transferência de conhecimentos da solução, de modo a capacitar a equipe técnica do CONTRATANTE para a utilização de todos os recursos operacionais disponíveis da solução.

1.9.33. A Contratada deverá apresentar um Plano de Capacitação no prazo máximo de 20 (vinte) dias corridos após assinatura do Termo de Contrato, onde deverá constar no mínimo:

1.9.33.1. conteúdo programático;

1.9.33.2. carga horária;

1.9.33.3. que lhe confira(m) as competências necessárias para ministrar a capacitação – neste caso, o profissional deverá ser certificado pelo fabricante da solução, e com experiência comprovada nos produtos fornecidos.

1.9.34. Após a apresentação formal da ementa da capacitação, o CONTRATANTE poderá solicitar à Contratada a alteração do conteúdo mediante eventuais ajustes visando atender aos objetivos da capacitação na administração e uso da solução.

1.9.35. A transferência de conhecimentos só ocorrerá após agendamento prévio pela CONTRATANTE, com antecedência mínima de 15 (quinze) dias.

1.9.36. A transferência de conhecimentos deverá ser executada em no máximo 15 (quinze) dias corridos após a implantação da solução e disponibilização das licenças no ambiente tecnológico do CONTRATANTE, sem obrigatoriedade de ser treinamento oficial do Fabricante.

1.9.37. A transferência de conhecimentos deverá ser ministrada com carga horária mínima de 20 (vinte) horas, para o quantitativo mínimo de 6 (seis) participantes, a serem selecionados pelo CONTRATANTE.

1.9.38. A transferência de conhecimentos não poderá ser meramente expositiva; devendo ser focada no uso prático de toda a solução implementada no ambiente tecnológico do Órgão.

1.9.39. A transferência de conhecimentos deverá ser ministrada preferencialmente nas dependências do CONTRATANTE, em data e horário conforme cronograma a ser estabelecido em comum acordo entre as partes.

1.9.40. Caberá ao CONTRATANTE providenciar o ambiente onde será realizada a transferência de conhecimentos, cabendo à Contratada informar da necessidade de se providenciar recursos necessários para o evento (projetor, computadores, notebooks etc.).

1.9.41. O curso a ser ofertado não possui obrigatoriedade de ser oficial do Fabricante da solução, contudo deve ser baseado em documentação oficial ou autorizado por ele.

1.9.42. Caberá à Contratada prover o material didático individual, podendo este ser oficial do Fabricante ou baseado neste.

1.9.43. O idioma a ser adotado deverá ser preferencialmente o português do Brasil.

1.9.44. A transferência de conhecimentos provida deverá abordar todos os componentes da solução fornecida, devendo ainda estar de acordo com a utilização da solução instalada no ambiente tecnológico do CONTRATANTE, abrangendo, no mínimo, mas não se restringindo, os seguintes tópicos:

1.9.44.1. conceitos e características das funcionalidades do produto e seus modos de funcionamento;

1.9.44.2. instalação e configuração do appliance físico, incluindo configuração das interfaces de rede, implementação de updates, configurações em geral, etc.;

1.9.44.3. gerenciamento da solução, incluindo monitoramento de eventos, configuração e utilização da gerência do produto, geração de relatórios com informações do trafego de rede, dentre outras funcionalidades de administração da solução;

1.9.44.4. configurações de todas as funcionalidades disponíveis na solução, políticas de segurança, identificação e prevenção dos principais ataques, monitoramento e relatórios, logs, mitigação de ataques, criptografia e segurança de dados, dentre outras funcionalidades;

1.9.44.5. solução de problemas (“troubleshooting”, log de eventos, etc.).

1.9.45. Os custos referentes ao deslocamento, hospedagem e diárias dos instrutores deverão estar previstos pela Contratada na elaboração de sua proposta comercial.

1.9.46. Para o caso de possíveis medidas de segurança adotadas em relação à pandemia do novo coronavírus, este treinamento poderá opcionalmente ser realizado por meio de Ensino a Distância (EAD) ou transmissão em tempo real, por meio de videoconferência (desde que permita a interação entre participante e instrutor em tempo real), onde a plataforma utilizada e a respectiva gravação do conteúdo ministrado será de responsabilidade exclusiva da Contratada que, ao final do repasse, deverá fornecer a mídia gravada em formato eletrônico.

1.9.47. Neste caso, a plataforma utilizada será de responsabilidade exclusiva da Contratada. Todavia tal modalidade de treinamento deverá, além de permitir a interação entre participante e instrutor em tempo real, igualmente contemplar todas as exigências mínimas previstas no modelo presencial quanto da utilização de todos os recursos da solução implantada no ambiente do Órgão.

1.9.48. O CONTRATANTE resguardar-se-á do direito de acompanhar e avaliar a capacitação mediante utilização de formulário de avaliação próprio baseado nos requisitos técnicos mínimos exigidos, que medirá o nível de satisfação dos participantes do CONTRATANTE em relação à metodologia, instrutoria, qualidade dos recursos e materiais didáticos, e à carga horária efetiva, em escala de 0 (zero) até 10 (dez) pontos, cujo resultado final será a média aritmética simples obtida a partir da soma das notas de cada item avaliado dividida pela quantidade numérica destes itens avaliados pelos participantes.

1.9.49. no caso de avaliação com média global igual ou superior a 7 (sete) pontos, a transferência de conhecimentos será considerada aprovada e finalizada;

1.9.50. para uma avaliação com média global abaixo de 7 (sete) pontos, a transferência de conhecimentos será considerada insuficiente, devendo a Contratada efetuar reestruturação e/ou ajustes necessários e realizar o curso novamente, sem nenhum ônus adicional ao CONTRATANTE.

1.9.51. Ao término da capacitação, a Contratada deverá emitir certificado individual de conclusão, para todos os participantes, sem nenhum ônus adicional ao CONTRATANTE.

- **LOTE II**
- **ITEM 4: EQUIPAMENTO PARA A INTERCEPTAÇÃO DO TRÁFEGO**

1.10. **CARACTERÍSTICAS TÉCNICAS**

1.10.1. O equipamento ofertado deverá atender a todas as exigências aqui descritas integralmente.

1.10.2. Com o intuito de garantir a homologação do equipamento ofertado, no que tange o seu padrão de qualidade, de segurança, de compatibilidade eletromagnética, de não agressão ao meio ambiente e de funcionalidade técnica regulamentada, deverá ser anexada a sua certificação oficial ANATEL, atendendo assim a resolução 715/2019 da Agência.

1.10.3. O equipamento ofertado deverá possuir funcionalidades e hardware específicos para este propósito de agregação, regeneração, filtragem e modificação/transformação do tráfego, não sendo aceita soluções similares, como: switches, roteadores, firewalls, balanceadores, servidores, soluções híbridas e etc.

1.10.4. São apresentadas, a seguir, as especificações técnicas mínimas a serem ofertadas referentes ao objeto. Os termos “possuir”, “permite/permitir”, “implementar” e “é” implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

1.10.5. Toda a oferta de softwares, mesmo quando condicionados a módulos físicos/hardwares específicos, deverá ser fornecida na modalidade de subscrição.

1.10.5.1. Não serão admitidas ofertas de licenças utilizadas na prestação de serviços – modalidade em que ao término da vigência de garantia da licença ela retorna ao fornecedor.

1.10.5.2. As licenças apresentadas deverão ser fornecidas em nome da CONTRATANTE.

1.10.5.3. Deverá possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas de “rede”, “rede inline”, “ferramenta” e portas de “ferramenta inline”.

1.10.5.4. Entende-se por portas de “rede”, todas as portas que serão responsáveis por receber a cópia do tráfego através dos TAPs/SPANs.

1.10.5.5. Entende-se por portas de “ferramenta”, todas as portas que serão responsáveis por encaminhar o tráfego, seja ele já filtrado e/ou modificado, para as ferramentas que serão conectadas a solução de interceptação do tráfego.

1.10.5.6. Entende-se por portas de “rede inline”, todas as portas que serão responsáveis por se conectar de forma inline (entre os enlaces) na rede de produção.

1.10.5.7. Entende-se por portas de “ferramenta inline”, todas as portas que serão responsáveis por encaminhar o tráfego de produção, selecionado através dos filtros ou não, para as ferramentas inline que serão conectadas a solução de interceptação do tráfego.

1.10.6. O equipamento deve estar em conformidade com o padrão RoHS.

1.10.7. Deverá possuir módulos de ventilação hot swappable;

1.10.8. Possuir ventilação "front-to-back", ou seja, a saída de ar quente deve acontecer pela traseira do equipamento.

1.10.9. Deverá possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable.

1.10.10. Deverá vir acompanhada de seus respectivos cabos de energização padrão C13-C14, de no mínimo 1,00m (um metro).

1.10.11. Deverá ser fornecido com o máximo de fontes de alimentação suportadas no equipamento. As fontes deverão ser do tipo AC redundantes, internas ao chassi e do tipo hot-swappable.

1.10.12. Deverá suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento.

1.11. **PROCEDIMENTOS PARA A OPERACIONALIZAÇÃO DA SOLUÇÃO DO LOTE 02**

1.11.1. Será de responsabilidade da CONTRATADA executar os seguintes procedimentos de instalação da solução adquirida:

1.11.1.1. Executar o levantamento de requisitos de rede, incluindo as informações de interfaces, portas lógicas, fluxo do tráfego e protocolos que deverão ser associados a plataforma.

1.11.1.2. Apoiar a CONTRATANTE na definição da arquitetura da solução, a qual deverá incluir a topologia, os pontos de coleta e o direcionamento do tráfego.

1.11.1.3. Executar todos os procedimentos de montagem da solução em rack, de cabeamento e de energização para a inicialização correta da solução.

1.11.1.4. Aplicar todas as licenças e atualizar o firmware da solução para a versão mais estável.

1.11.1.5. Executar todas as configurações para o gerenciamento remoto da solução, incluindo a configuração de usuário administrador, SNMP, Syslog e NTP.

1.11.1.6. Construir 3 (três) regras de mapeamento do fluxo de tráfego entre contextos de coleta de dados.

1.11.2. Após o término dos procedimentos de configuração, a CONTRATADA deverá:

1.11.2.1. Executar os testes de passagem de tráfego para validar o fluxo correto de informações.

1.11.2.2. Validar as regras de fluxo de dados conforme orientado pela CONTRATANTE.

1.11.2.3. Executar os testes de entrega de tráfego para as ferramentas interconectadas na solução.

1.11.2.4. Executar testes de alta disponibilidade na solução – quando factível.

1.11.2.5. A CONTRATADA deverá emitir relatório As-Built de todos os procedimentos executados, incluindo diagramas lógicos e físicos.

1.11.2.6. Os procedimentos deverão ser executados presencialmente, nas mesmas dependências as quais forem instaladas as soluções, conforme determinado pela CONTRATANTE.

1.12. **REPASSE DE CONHECIMENTO NA SOLUÇÃO DO LOTE 02**

1.12.1. Após o término dos procedimentos de instalação, a CONTRATADA deverá executar repasse de conhecimento na solução implantada, sendo admitido o uso da própria solução já configurada para a execução do repasse.

1.12.2. O repasse deverá possuir duração mínima de 16 (dezesseis) horas, sendo admitida a sua divisão em 2 (dois) ou 4 (quatro) dias de repasse.

1.12.3. O serviço poderá ser executado pelo mesmo profissional responsável pelos procedimentos de instalação, ou por outro profissional certificado na solução.

1.12.4. O repasse deverá ser executado em formato on-line síncrono, de modo remoto.

1.12.5. O repasse de conhecimento deverá abordar os seguintes tópicos, minimamente:

1.12.6. Visão geral da arquitetura da solução:

1.12.6.1. Componentes da solução;

1.12.6.2. Topologias comuns;

1.12.6.3. Fluxo do tráfego.

1.12.7. Acesso e gerenciamento:

1.12.7.1. Interface de gerenciamento e configuração da solução;

1.12.7.2. Procedimentos de backup das configurações;

1.12.7.3. Configuração de serviços internos de rede da solução.

1.12.8. Configurações de rede:

1.12.8.1. Portas e interfaces;

1.12.8.2. Regras de filtro de tráfego;

1.12.8.3. Regras de encaminhamento;

1.12.8.4. Aplicação de funcionalidades correlatas.

1.12.9. Operação:

1.12.9.1. Depuração e troubleshooting;

1.12.9.2. Abertura de chamados;

1.12.9.3. Gerenciamento de licenças.

1.13. **CARACTERÍSTICAS DE GERENCIAMENTO DA SOLUÇÃO**

1.13.1. Deverá possuir, no mínimo, 1 (uma) interface exclusiva ao gerenciamento remoto do equipamento.

1.13.1.1. As interfaces deverão vir acompanhadas de seus respectivos cabos UTP de, no mínimo, 1,0m (um metro) e com conectores RJ-45.

1.13.2. Deverá permitir configuração customizada baseadas nos perfis de acesso (RBAC - Role Base Access Control).

1.13.3. Deverá implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.

1.13.4. Deverá possuir suporte a MIB II.

1.13.5. Deverá implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.

1.13.6. Deverá suportar SNMP trap sobre IPv6.

1.13.7. Deverá permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface de gerenciamento.

1.13.8. Deverá permitir a gravação de log externo (syslog).

1.13.9. Deverá permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação

1.13.10. Deverá possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como estatísticas de utilização e log de eventos.

1.13.11. Deve suportar configuração total da solução através de console local RS-232 ou RJ-45.

1.13.12. Deve possuir gerenciamento através de interface Web (HTTPS) ou CLI.

1.13.13. Deverá implementar o protocolo NTP (Network Time Protocol).

1.13.14. Deverá implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+, RADIUS e LDAP.

1.13.15. Deve suportar IPv6 para TACACS+.

1.13.16. Deverá implementar o protocolo SSHv2 para acesso à interface de linha de comando.

1.13.17. Deverá proteger a interface de comando do equipamento através de senha.

1.13.18. Possuir gerenciador em um único ponto central para orquestrar todo os elementos físicos, virtuais, em nuvem e containers que compõem o projeto. A solução deve permitir o gerenciamento de todos os componentes da solução, incluindo appliances físicos e virtuais, nuvem e containers.

1.14. **CARACTERÍSTICAS DE SEGURANÇA**

1.14.1. A solução deverá implementar as seguintes configurações para agregação e encaminhamento de pacotes das portas de Rede para as portas de Ferramentas, tanto para os fluxos “Out-of-Band” (Cópia de Tráfego) quanto para Inline, respectivamente:

1.14.1.1. Uma para uma (1 : 1);

1.14.1.2. Uma para várias (1 : N) - Com suporte ao balanceamento;

1.14.1.3. Várias para uma (N : 1);

1.14.1.4. Várias para várias (N : N) - Com suporte ao balanceamento.

1.14.2. Deverá permitir criar filtros (regras) baseados em, no mínimo, os seguintes campos:

1.14.2.1. Endereços MAC de origem e destino;

1.14.2.2. Endereço IPv4 de origem/destino;

1.14.2.3. Portas TCP e UDP de origem e destino;

1.14.2.4. VLAN ID;

1.14.2.5. Ethertype;

1.14.2.6. IPFrag;

1.14.2.7. TTL;

1.14.2.8. TOS;

1.14.2.9. Protocol;

1.14.2.10. TCP Control Mask/Bits;

1.14.2.11. DSCP;

1.14.2.12. Versão do Protocolo IPv4 e IPv6;

1.14.2.13. Endereço IPv6 de origem/destino.

1.14.3. Deverá permitir a inserção e remoção de novos filtros (regras) sem a necessidade de reiniciar o(s) equipamento(s), ou seja, a aplicação destes filtros (regras) deverá acontecer em tempo real.

1.14.4. Deve suportar overlapping de filtros (regras), ou seja, utilização conjunta de filtros de entrada (ingress) e filtros de saída (egress).

1.14.5. A solução deverá implementar funcionalidade Mesh/Cluster.

1.14.5.1. O Mesh/Cluster deverá permitir a configuração e gerenciamento de 2 (dois) ou mais equipamentos como um único equipamento lógico. Não serão aceitas soluções em cascateamento (empilhamento) para o atendimento desta funcionalidade.

1.14.5.2. A solução deverá suportar, no mínimo, 30 (trinta) equipamentos em modo Mesh/Cluster.

1.14.6. O Mesh/Cluster deverá permitir a configuração de todos os Agregadores a partir de uma única interface WEB (HTTPS) e CLI.

1.14.7. A funcionalidade de Mesh/Cluster deverá suportar a criação de 1 (um) ou mais filtros (regras) que se utilizem de “portas de rede” em um equipamento físico e direcionem este tráfego para “portas de ferramenta” localizadas em outro equipamento físico, independentemente da quantidade de ativos de rede e/ou de processamento entre estes equipamentos. Não serão aceitas soluções em cascateamento/empilhadas para o atendimento deste item.

1.14.8. A funcionalidade de Mesh/Cluster deve suportar arquitetura conhecida como Spine/Leaf, permitindo balanceamento do tráfego entre os Leafs e os Spines e adicionando redundância a solução em caso de falha de um dos equipamentos.

1.14.9. Deve suportar o conceito de FABRIC que permite a criação de filtros que se estendem por múltiplos equipamentos ou mesh/clusters de equipamentos.

1.14.10. Deve permitir a configuração de circuitos entre mesh/clusters de equipamentos, permitindo que o tráfego recebido em um cluster seja entregue para uma ferramenta em outro cluster.

1.15. **REDUNDÂNCIA E ALTA DISPONIBILIDADE**

1.15.1. A solução deverá operar em alta disponibilidade e suportar instalação em redes diferentes.

1.15.1.1. Serão aceitos sistemas de redundância que necessitem de operação manual, desde que não sejam necessários quaisquer outros procedimentos manuais de sincronização de configuração ou backup entre os servidores.

1.15.2. Caso o equipamento principal sofra uma interrupção, os novos tráfegos não deverão ser bloqueados, isto é, deve permitir o bypass sem prejudicar o acesso do cliente.

1.16. **FUNCIONALIDADES PARA O TRÁFEGO INTERCEPTADO EM LINHA**

1.16.1. O equipamento deve suportar instalação sem necessidade de reconfiguração de roteadores e switches, quando utilizado no modo de operação inline (em linha).

1.16.2. O equipamento deve suportar, de forma simultânea e em interfaces distintas, os modos:

1.16.2.1. TAP/SPAN (Cópia de Tráfego);

1.16.2.2. Inline (Tráfego de Produção);

1.16.3. A solução deverá ser capaz de configurar a sequência das ferramentas inline (serial), quando possuir 2 (duas) ou mais ferramentas, pela qual os pacotes deverão ser encaminhados sequencialmente quando o agregador funcionar de forma online.

1.16.4. A solução deverá ser capaz de configurar um grupo de ferramentas inline (Paralelo), quando possuir 2 (duas) ou mais ferramentas, pela qual os pacotes deverão ser balanceados entre as ferramentas quando o agregador funcionar de forma Inline.

1.16.5. A solução deverá permitir a configuração conjunta das funcionalidades serial e paralelo, permitindo criar uma sequência serial de ferramentas que estão em paralelo.

1.16.6. A solução deverá permitir que ferramentas inline em modo standalone (operação individual), serial e paralelo, possam ter a flexibilidade de receber somente o tráfego de interesse, sem impacto entre elas e sem a necessidade de solução de contorno físico.

1.16.6.1. Por exemplo, uma ferramenta precisa receber todo o tráfego e uma outra ferramenta necessita receber apenas tráfego WEB, nesse tipo de cenário as ferramentas devem receber o tráfego desejado sem necessidade de arranjos físicos e sem impactar o tráfego uma da outra.

1.16.7. A solução deve suportar heartbeat para monitoramento da saúde das ferramentas, quando utilizadas de forma inline, permitindo detectar e remover somente a ferramenta que apresentar falha, sem causar impacto no fluxo de dados das outras ferramentas e no tráfego de rede.

1.16.8. A solução deve suportar heartbeat negativo, que permite utilizar um pacote específico para a geração do tráfego de checagem, no entanto, este pacote deve ser bloqueado pela ferramenta inline, não retornando novamente para a solução de interceptação. Caso este pacote retorne a ferramenta inline será considerada com falha e deverá ser removida sem impacto na rede e nos fluxos de dados.

1.16.9. A solução, quando utilizada em modo inline, deve permitir remover uma ou mais ferramentas da sequência do tráfego sem causar impacto no tráfego da rede. Esta funcionalidade tem como principal objetivo remover ferramentas para atualização e para fins de troubleshooting, sem causar interrupção de rede.

1.17. **TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO**

1.17.1. Deve suportar funcionalidade túnel (Tunnel), que permite encapsulamento e desencapsulamento de tráfego entre 2 (dois) equipamentos através de redes L3 (roteadas).

1.17.2. A funcionalidade de túnel deve suportar o encapsulamento e o desencapsulamento utilizando protocolo L2GRE ou similar, permitindo transportar o tráfego encapsulado através de diferentes redes L3.

1.17.3. Deve suportar o balanceamento de carga dos pacotes de encapsulamento IPv6 L2GRE.

1.17.4. A solução deverá suportar balanceamento entre diferentes túneis, permitindo utilizar duas ou mais ferramentas da mesma solução como destino para todo o tráfego encapsulado.

1.18. **CARACTERÍSTICAS DE HARDWARE**

1.18.1. O equipamento deve ser baseado em appliance modular suportando montagem em rack de 19”, com altura de no máximo 1-RU (uma unidade de altura), com fornecimento dos respectivos conjuntos de fixação.

1.18.2. O appliance deverá ser fornecido com suas devidas licenças, de funcionalidades ou de sistema operacional, que permitem a execução das técnicas previstas nesta especificação técnica.

1.18.3. O licenciamento deverá ser ofertado na modalidade de subscrição, não sendo admitidas ofertas de licenças empregadas na prestação de serviços.

1.19. **CARACTERÍSTICAS DE DESEMPENHO**

1.19.1. O equipamento deverá possuir a capacidade de processamento de, no mínimo, 1.800 Gbps (mil e oitocentos gigabits por segundo) de tráfego agregado para aplicação dos filtros (regras) descritos nesta especificação.

1.19.1.1. Esta capacidade poderá ser alcançada através da adição de módulos ou licenças.

1.19.2. O equipamento deverá suportar, no mínimo, 36.000 (trinta e seis mil) filtros (regras) de entrada e saída por modulo.

1.20. **INTERFACES DE COMUNICAÇÃO**

1.20.1. O equipamento deverá ser fornecido com, no mínimo, 8 (oito) interfaces padrão Ethernet 25/10/1Gbps SFP.

1.20.1.1. O equipamento deverá ser fornecido com 4 (quatro) transceivers 25Gbps SFP28 de curto alcance, com suas respectivas fibras OM4 UPC de 5,0m e conectores LC. O tipo de conector da fibra será definido durante a fase de implementação da solução.

1.20.2. O equipamento deverá ser fornecido com 4 (quatro) interfaces padrão Ethernet 100/40Gbps QSFP28.

- **ITEM 05 – LICENCIAMENTO DE DESDUPLICAÇÃO DO TRÁFEGO**

1.21. **CARACTERÍSTICAS DE LICENCIAMENTO**

1.21.1. O licenciamento fornecido deverá permitir o emprego das técnicas de desduplicação aqui exigidas, através do emprego delas no equipamento de interceptação de tráfego ofertado, ampliando sua capacidade técnico operacional.

1.21.1.1. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.21.2. O licenciamento deverá ser ofertado na modalidade de subscrição, não sendo admitidas ofertas de licenças empregadas na prestação de serviços – modalidade em que ao término da vigência de garantia a licença retorna ao fornecedor.

1.22. **CARACTERÍSTICAS DE DESEMPENHO**

1.22.1. O equipamento deverá possuir capacidade de processamento agregado de, no mínimo, 116 (cento e dezesseis) Gbps de throughput, específico para o processamento de Deduplicação, dado que o licenciamento fora instalado no equipamento.

1.23. **CARACTERÍSTICAS DE REDUÇÃO DO TRÁFEGO**

1.23.1. Deve implementar a funcionalidade Packet De-Duplication (De-duplicação de Pacotes), enviando somente uma única cópia do pacote para as Ferramentas.

1.23.2. A funcionalidade de Packet De-Duplication deve implementar de-duplicação de pacotes IPv4, IPv6 e pacotes sem IP, devendo levar em consideração o Payload e os cabeçalhos ethernet.

1.23.3. A funcionalidade Packet De-Duplication deve detectar pacotes duplicados recebidos em diferentes portas ou módulos do(s) equipamento(s), inclusive se utilizado em modo Mesh/Cluster, detectando pacotes duplicados entre diferentes portas, módulos e equipamentos.

1.23.4. A funcionalidade Packet De-Duplication deve permitir habilitar ou desabilitar a inspeção de, no mínimo, os seguintes campos para avaliar se é um pacote duplicado ou não:

1.23.4.1. IPv4 ToS;

1.23.4.2. IPv6 TC;

1.23.4.3. Número da Sequência TCP;

1.23.4.4. VLAN ID.

- **ITEM 06 – LICENCIAMENTO AVANÇADO DE DESCRIPTAÇÃO DO TRÁFEGO**

1.24. **CARACTERÍSTICAS DE LICENCIAMENTO**

1.24.1. O licenciamento fornecido deverá permitir o emprego das técnicas de criptografia e descriptografia aqui exigidas, através do emprego delas no equipamento de interceptação de tráfego ofertado, ampliando sua capacidade técnico operacional.

1.24.1.1. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.24.2. O licenciamento deverá ser ofertado na modalidade de subscrição, não sendo admitidas ofertas de licenças empregadas na prestação de serviços – modalidade em que ao término da vigência de garantia a licença retorna ao fornecedor.

1.25. **CARACTERÍSTICAS DE DESEMPENHO**

1.25.1. Deverá implementar um throughput exclusivo de tráfego de processamento de filtro de SSL decriptografado de, no mínimo, 4.7 (quatro vírgula sete) Gbps, respeitando as demais condições técnicas previstas para segurança da informação.

1.26. **CARACTERÍSTICAS DE SEGURANÇA DA INFORMAÇÃO**

1.26.1. Deve implementar a funcionalidade SSL Decryption através de função Man-In-The-Middle e também somente cópia do tráfego.

1.26.2. A descriptografia deve ser baseada no handshake SSL/TLS e não através de portas pré-definidas.

1.26.3. O equipamento deve permitir importação de no mínimo 1.000 (hum mil) certificados em formato PKCS #12 ou PEM.

1.26.4. Implementar no mínimo de 8,5 mil novas conexões SSL por segundo, utilizando cifra ‘TLS_RSA_WITH_AES_128_CBC_SHA256’ e criptografia RSA de 2048 bits;

1.26.5. Implementar no mínimo 100 mil conexões SSL simultâneas utilizando criptografia de 2048 bits;

1.26.6. O equipamento deve implementar, no mínimo, os seguintes algoritmos de troca de chaves com autenticação:

1.26.6.1. RSA;

1.26.6.2. DHE;

1.26.6.3. DHE_RSA;

1.26.6.4. ECDHE com PFS (Perfect Forward Secrecy)

1.26.6.5. ECDHE_RSA;

1.26.6.6. ECDHE_ECDSA.

1.26.7. O equipamento deve implementar, no mínimo, os seguintes métodos de autenticação de mensagem:

1.26.7.1. SHA;

1.26.7.2. SHA256;

1.26.7.3. SHA384;

1.26.7.4. POLY1305.

1.26.8. Deverá implementar Host Categorization, permitindo selecionar tráfegos que não serão descriptografados, como dados financeiros por exemplo.

1.26.9. A funcionalidade SSL Decryption se suportar, no mínimo, os seguintes protocolos:

1.26.9.1. SSL 3;

1.26.9.2. TLS 1.0;

1.26.9.3. TLS 1.1;

1.26.9.4. TLS 1.2;

1.26.9.5. TLS 1.3.

1.26.10. Deve suportar chaves de 1024 bits, 2048 bits e 4096 bits.

1.26.11. O equipamento deve suportar, no mínimo, as seguintes cifras de criptografia:

1.26.11.1. AES_128_CBC;

1.26.11.2. AES_256_CBC;

1.26.11.3. AES_256_GCM;

1.26.11.4. CHACAH20;

1.26.11.5. Camellia128;

1.26.11.6. Camellia256;

1.26.11.7. DES_CBC;

1.26.11.8. DES_EDE_CBC;

1.26.11.9. SEED;

1.26.11.10. IDEA;

1.26.11.11. Chacah20-Poly1305.

1.27. **ALTA DISPONIBILIDADE**

1.27.1. Quando implementado em alta disponibilidade, em caso de falha de um dos equipamentos, a inspeção SSL deverá ser realizada pelo outro equipamento.

1.27.2. Deve fazer ou permitir a opção de bypass do tráfego caso falhe o TLS handshake.

1.27.3. Implementar funcionalidade conhecida como “Fail-Safe” através do uso de bypass, que mesmo em caso de perda de energia, os links interceptados da rede continuem ativos, não gerando indisponibilidade de rede.

1.27.4. Em caso de composição com bypass externo, este deve ser obrigatoriamente do mesmo fabricante do restante da solução, não sendo permitido a sua composição com bypass OEM ou de terceiros;

1.27.5. A solução deve permitir a alteração do modo de operação sem causar interrupção de rede da ferramenta inline para “simulação inline” sem causar interrupção de rede, de modo que a ferramenta entenda que está inline mas está recebendo apenas uma cópia dos dados que foram encaminhados para rede.

- **ITEM 07 – LICENCIAMENTO AVANÇADO DE ANÁLISE DE APLICAÇÕES**

1.28. CARACTERÍSTICAS DE LICENCIAMENTO

1.28.1. O licenciamento fornecido deverá permitir o emprego das técnicas de análise de aplicações aqui exigidas, através do emprego delas no equipamento de interceptação de tráfego ofertado, ampliando sua capacidade técnico operacional.

1.28.1.1. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.28.2. O licenciamento deverá ser ofertado na modalidade de subscrição, não sendo admitidas ofertas de licenças empregadas na prestação de serviços – modalidade em que ao término da vigência de garantia a licença retorna ao fornecedor.

1.29. **CARACTERÍSTICAS DE DESEMPENHO**

1.29.1. Deverá implementar um throughput exclusivo de tráfego de processamento de filtro de aplicações de, no mínimo, 65 (sessenta e cinco) Gbps, dado que o licenciamento fora instalado no equipamento.

1.30. **CARACTERÍSTICAS DE SEGURANÇA DA INFORMAÇÃO**

1.30.1. Deve implementar a funcionalidade DPA (Deep Packet Analysis), que permita criar filtros (regras) que identifiquem qualquer informação dentro do pacote, desde o cabeçalho até o Payload.

1.30.2. A funcionalidade DPA deve permitir a criação de filtros (regras) utilizando linguagem de programação Perl ou RegEx.

1.30.3. A funcionalidade DPA deve permitir a criação de filtros (regras) utilizando uma string.

1.30.4. A funcionalidade DPA deve permitir a criação de filtros (regras) que façam "match" nos campos ethernet mesmo quando a informação estiver encapsulada por outros protocolos, como FCoE.

1.30.5. Deve implementar funcionalidade de Application Aware (App-Aware), que permite compreender uma sessão completa de um fluxo de dados e encaminhar/bloquear todos os pacotes subsequentes desta sessão para as Ferramentas.

1.30.6. A funcionalidade App-Aware deve implementar a utilização de buffer da sessão, permitindo armazenar, no mínimo, os 20 pacotes iniciais da sessão, para que nos casos onde o padrão da sessão for detectado após o handshake da sessão, todos os pacotes anteriores também sejam encaminhados para as Ferramentas.

1.30.7. Deve implementar a filtragem de tráfego com base na visibilidade da camada de aplicação, permitindo a identificação bidirecional do tráfego na camada 7 do modelo OSI através de funcionalidade de DPI (Deep Packet Inspection).

1.30.8. Deve implementar a identificação de, no mínimo, 3500 aplicações agrupadas por famílias ou grupos de aplicações tais como YouTube, Whatsapp e Gmail.

1.30.9. Deve implementar a definição de assinaturas para aplicações customizadas, incluindo protocolos e extensões proprietárias.

1.30.10. Após a identificação do tráfego com base na aplicação, a solução deve suportar a criação de filtros (regras) de encaminhamento e replicação de tráfego.

- **ITEM 08 – LICENCIAMENTO AVANÇADO DE ANÁLISE DE METADADOS**

1.31. **CARACTERÍSTICAS DE LICENCIAMENTO**

1.31.1. O licenciamento fornecido deverá permitir o emprego das técnicas de análise de metadados aqui exigidas, através do emprego delas no equipamento de interceptação de tráfego ofertado, ampliando sua capacidade técnico operacional.

1.31.1.1. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.31.2. O licenciamento deverá ser ofertado na modalidade de subscrição, não sendo admitidas ofertas de licenças empregadas na prestação de serviços – modalidade em que ao término da vigência de garantia a licença retorna ao fornecedor.

1.32. **CARACTERÍSTICAS DE DESEMPENHO**

1.32.1. Deverá implementar um throughput exclusivo de tráfego de processamento de metadados de, no mínimo, 22 (vinte e dois) Gbps, dado que o licenciamento fora instalado no equipamento.

1.33. **CARACTERÍSTICAS DE SEGURANÇA DA INFORMAÇÃO**

1.33.1. Deve gerar, no mínimo, os seguintes metadados para prover informações superiores à da camada de rede, quando utilizando IPFIX/CEF:

1.33.1.1. HTTP Method;

1.33.1.2. HTTP Response Code

1.33.1.3. HTTP Version;

1.33.1.4. HTTP Host;

1.33.1.5. HTTP User Agent;

1.33.1.6. DNS Query Name;

1.33.1.7. DNS Query Type

1.33.1.8. DNS Response Code;

1.33.1.9. DNS Response TTL;

1.33.1.10. DNS Response Name;

1.33.1.11. DNS Response IPv6/IPv4;

1.33.1.12. SSL Certificate Issuer;

1.33.1.13. SSL Certificate CN;

1.33.1.14. SSL Version;

1.33.1.15. SSL Cipher.

1.33.1.16. Mysql Query, Mysql login, Mysql Error;

1.33.1.17. Modbus length, Modbus events, Modbus error_code;

1.33.1.18. RDP Username ASCII;

1.33.1.19. RDP Encryption Level;

1.33.1.20. RDP Security Protocol;

1.33.1.21. TCP RTT;

1.33.1.22. TCP RTT App;

1.33.1.23. TCP Loss bytes;

1.33.1.24. TCP Retransmission bytes; e

1.33.1.25. TCP Wrong CRC.

- **ITEM 09 – MÓDULO DE EXPANSÃO DO PROCESSAMENTO**

1.34. **CARACTERÍSTICAS TÉCNICAS**

1.34.1. O objeto ofertado deverá corresponder a 1 (um) módulo o qual possibilita a expansão da quantidade de processamento do tráfego de rede dos equipamentos de interceptação de tráfego.

1.34.2. O módulo deverá fornecer a capacidade de processamento de tráfego de, no mínimo, 80 Gbps (oitenta gigabits por segundo).

1.34.2.1. Serão admitidos módulos de processamento que são acoplados ao equipamento de interceptação do tráfego ofertado.

1.34.2.2. Caso a solução ofertada não possua módulo de expansão de processamento, será admitido o fornecimento de equipamento de interceptação de tráfego capaz de processar o tráfego exigido.

1.34.2.3. Nessas condições, o equipamento deverá respeitar as condições exigidas no equipamento de interceptação de tráfego anteriormente descrito, incluindo interfaces, padrão SFP28 ou QSFP28 em quantidades suficientes para comportar o processamento de tráfego exigido.

1.34.2.4. Caberá a CONTRATADA fornecer todo o serviço de integração do módulo extra com a solução contratada e garantir seu funcionamento conjunto.

1.34.3. O módulo fornecido deverá suportar, minimamente, as seguintes funcionalidades de interceptação de tráfego:

1.34.3.1. Emprego das técnicas de redução do tráfego através da execução das funcionalidades de De-duplicação supracitadas;

1.34.3.2. Emprego das técnicas de descriptografia do tráfego através da execução das funcionalidades supracitadas;

1.34.3.3. Emprego das técnicas de análise do tráfego de aplicações através da execução das funcionalidades supracitadas;

1.34.4. O módulo deverá permitir a configuração de quais funcionalidades serão aplicadas nele, conforme a vontade do administrador da solução e a capacidade da solução em executar rotinas concomitante de processamento do tráfego.

1.34.5. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

- **ITEM 10 – MÓDULO DE EXPANSÃO PARA A CAPTURA DO TRÁFEGO “INLINE”**

1.35. **CARACTERÍSTICAS TÉCNICAS**

1.35.1. O objeto ofertado deverá corresponder a 1 (um) módulo o qual possibilita a expansão da quantidade de interfaces de interceptação do tráfego de rede dos equipamentos de interceptação de tráfego.

1.35.1.1. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.36. **INTERFACES DE COMUNICAÇÃO**

1.36.1. Deverá fornecer, no mínimo, 6 (seis) pares de interfaces Ethernet 10Gb para a interconexão de fibras padrão LC-LC, do tipo “by-pass”.

1.36.2. O módulo deverá ser do tipo “hot-swap”.

1.37. **ALTA DISPONIBILIDADE**

1.37.1. Em caso de não energização do módulo, a solução deverá permitir que o tráfego flua diretamente entre a origem e o destino, com funcionamento em modo físico de “by-pass” (sem interceptação do tráfego).

1.37.2. Em caso de energização do módulo, a solução deverá permitir o controle do tráfego via software, incluindo a interceptação do tráfego e a execução conjunta com ferramentas que recebem o tráfego “inline”.

1.37.3. Deverá permitir o uso do módulo em configurações de alta disponibilidade, correspondentes a, no mínimo, um par de equipamentos implantados, garantindo a operação contínua da solução caso um equipamento ou módulo perca sua energização.

- **ITEM 11 – LICENCIAMENTO PARA O GERENCIAMENTO CENTRALIZADO DA SOLUÇÃO**

1.38. **CARACTERÍSTICAS GERAIS DA PLATAFORMA**

1.38.1. O licenciamento deverá ser ofertado na modalidade de subscrição, não sendo admitidas ofertas de licenças empregadas na prestação de serviços – modalidade em que ao término da vigência de garantia a licença retorna ao fornecedor.

1.38.1.1. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.38.2. A solução de gerenciamento centralizado deverá ser implementada em servidores físicos ou servidores virtuais. A infraestrutura base de sustentação da plataforma será fornecida pela CONTRATANTE.

1.38.3. No caso de fornecimento de plataforma virtualizada:

1.38.3.1. A solução deverá ser compatível com, no mínimo, os hypervisors VMware e Hyper-V.

1.38.3.2. A solução deverá ser fornecida conforme suas quantidades mínimas que garantem a alta disponibilidade do gerenciamento da plataforma.

1.38.3.3. A solução deverá estar dimensionada para comportar o gerenciamento de, no mínimo, 5 (cinco) equipamentos interceptadores de tráfego, possuindo recursos de processamento (vCPU e vRAM) em quantitativos suficientes para a correta operação da plataforma.

1.38.4. No caso de fornecimento de plataforma física:

1.38.4.1. Os equipamentos físicos, em alta disponibilidade, deverão ser fornecidos com todos os softwares necessários para prover os requisitos técnicos especificados, inclusive seus sistemas operacionais, sem qualquer ônus adicional e com garantia oficial da respectiva fabricante do sistema operacional.

1.38.4.2. No caso de servidores, a solução poderá adotar hardwares padrão de mercado, desde que atendam aos requisitos recomendados pela última versão do manual de instalação dos softwares utilizados, conforme demonstrado na comprovação técnica deste item.

1.38.4.3. Cada equipamento deverá possuir altura máxima de 1RU.

1.38.4.4. Todo hardware que compõe a solução deverá possuir alimentação elétrica de 110/240 V, 47 a 63 Hz, com chaveamento automático.

1.38.4.5. Todos os componentes de disponibilidade dos hardwares deverão ser redundantes (exceto por controladoras RAID), e hot-swap (exceto por slots PCIe, processadores e memórias).

1.39. **CARACTERÍSTICAS DE GERENCIAMENTO CENTRALIZADO**

1.39.1. Deverá ser fornecido um software capaz de controlar, administrar, gerenciar e monitorar a solução para interceptação do tráfego prevista nesta contratação.

1.39.2. O software deverá estar licenciado para gerenciar, no mínimo, 5 (cinco) equipamentos interceptadores de tráfego, físicos ou virtuais, da solução e permitir upgrades através da aquisição de licenças adicionais.

1.39.3. Possuir gerenciador em um único ponto central para orquestrar os elementos físicos e virtuais que compõem a solução de interceptação do tráfego.

1.39.4. A solução deve possuir uma interface gráfica e intuitiva com API abertas para simples customização de aplicações e integração com produtos de terceiros

1.39.5. A solução deve ser capaz de visualizar e gerenciar os dados e métricas coletadas em múltiplos segmentos monitorados em uma única console (centralizada), permitindo desta forma integração, maior segurança, escalabilidade, robustez e disponibilidade da solução.

1.39.6. Possuir interface gráfica para a criação dos filtros (regras), onde é possível selecionar as portas de Rede e as portas de Ferramentas, independentemente do equipamento físico. Os filtros (regras) criados para estes tráfegos deverão ser aplicados através desta mesma interface Web (HTTPS), facilitando a operação e entendimento dos fluxos.

1.39.7. A solução deve possibilitar a configuração de diferentes perfis de administradores. Deve ser possível ainda criar usuários com perfil de administração e outros de apenas visualização.

1.39.8. Deve permite gerar um token somente se você for um usuário autenticado e com base em seus privilégios de acesso a Gerência. Você pode copiar os tokens gerados da interface WEB, que pode ser usada para acessar as APIs REST.

1.39.9. A solução deve permitir que os usuários façam “drill down” a partir de visões de alto nível, orientadas a serviços, até visões técnicas com dados detalhados, que auxiliem na análise da causa raiz do problema.

1.39.9.1. Deve permitir a criação de topologias da solução de Visibilidade para todos os equipamentos ativos e gerenciáveis.

1.39.9.2. Deve permitir a identificação do status das portas dos dispositivos up ou down, tecnologia e velocidade das portas.

1.39.9.3. A solução deve permitir o inventário detalhado de atributos dos ativos da solução, atendendo, no mínimo, números seriais, módulos instalados, status do equipamento e versão de software instalado.

1.39.9.4. A solução deve permitir o armazenamento das configurações dos dispositivos.

1.39.9.5. A ferramenta deve permitir o agendamento da função de armazenamento de configuração de determinados elementos da rede. O agendamento deve ter periodicidade mínima de um dia.

1.39.9.6. Deve permitir o upgrade do sistema operacional ou Boot PROM dos dispositivos, unitariamente e para um grupo de dispositivos, inclusive podendo agendar um dia e horário para que este upgrade aconteça automaticamente.

1.39.9.7. A ferramenta deve permitir a execução do reset dos dispositivos.

1.39.9.8. A ferramenta deve permitir restaurar a configuração armazenada. Deve ser possível ainda aplicar essa configuração em um equipamento em processo de substituição.

1.39.9.9. Deve permitir a instalação dos TAPs virtuais a partir da console de gerência.

1.39.9.10. Deve possuir integração via API com a VMWare, para permitir cópia do tráfego entre as VMs mesmo em caso de mobilidade das VMs.

1.39.9.11. A solução deverá ser capaz de criar e configurar os filtros (regras) virtuais, ou seja, os filtros (regras) que serão aplicados dentro da solução virtual para que seja espelhado para fora do servidor somente o tráfego desejado.

1.39.9.12. A solução deverá possuir dashboards com, no mínimo, as seguintes informações:

1.39.9.13. Total de portas que estão perdendo pacotes;

1.39.9.14. Total de portas acima do limite de utilização, tanto portas de Rede como portas de Ferramenta;

1.39.9.15. TOP portas com maior utilização;

1.39.9.16. Visualização simplificada de todos os filtros (regras) aplicados, indicando as portas de Redes e Ferramentas.

- **ITEM 12 – INTERCEPTADOR DO TRÁFEGO VIRTUALIZADO AVANÇADO**

1.40. **CARACTERÍSTICAS DE LICENCIAMENTO E FORNECIMENTO**

1.40.1. Deverá ser fornecido no formato de appliance virtual, com seu licenciamento na modalidade de subscrição.

1.40.2. O licenciamento da solução deverá ser ofertado na modalidade de subscrição, não sendo admitidas ofertas de licenças empregadas na prestação de serviços – modalidade em que ao término da vigência de garantia a licença retorna ao fornecedor.

1.40.2.1. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.40.3. A solução entregue deverá estar licenciada para processar, no mínimo, 50 TB (cinquenta terabytes) de dados por dia.

1.41. **CARACTERÍSITCAS TÉCNICAS ESSENCIAIS DA SOLUÇÃO**

1.41.1. Deverá implementar a coleta de tráfego dentro do mundo virtual (tráfego entre VMs) através de Interceptadores Virtualizados ou Virtual TAPs.

1.41.2. Deverá se integrar, através de APIs específicas, com a VMware, OpenStack ou Nutanix, não sendo aceitas soluções que utilizem do modo promíscuo ou que façam qualquer alteração no kernel do Hypervisor, para todas as plataformas solicitadas.

1.41.3. Para a coleta de tráfego entre VMs deverá ser compatível com, no mínimo, as seguintes plataformas:

1.41.3.1. VMware 6.7 ou superior;

1.41.3.2. NSX-T 3.1 ou superior;

1.41.3.3. OpenStack;

1.41.4. Deverá suportar o monitoramento de múltiplos switches virtuais distribuídos da VMware simultaneamente.

1.41.5. Deverá suportar a identificação automática das VMs que devem ser monitoradas através das definições de regras de seleção do tráfego que deve ser monitorado, evitando que cada VM tenha que ser selecionada individualmente para monitoramento.

1.41.6. Deverá implementar a mobilidade das máquinas virtuais, de forma que quando ocorrer uma migração de uma VM para outro host, todas as políticas relacionadas a esta VM continuem sendo aplicadas sem a necessidade de reconfiguração manual.

1.41.7. Deve implementar a coleta de tráfego entre VMs de, no mínimo, 1.000 hypervisors e integração com, no mínimo, 10 vCenters.

1.41.8. Deverá permitir a visualização e monitoramento, através de um gerencia centralizada, de todos os appliances virtuais componentes da solução.

1.41.9. Deverá implementar a coleta de tráfego dentro do ambiente de conteinerização (Kubernetes) através de Container TAPs.

1.41.10. Deverá coletar o tráfego no ambiente de conteinerização independente da camada de rede de contêineres (CNI) utilizada.

1.41.11. Deverá coletar o tráfego de forma independente dos PODs em execução, não sendo necessária instrumentação dos PODs das aplicações.

1.41.12. Para coleta de tráfego entre PODs deverá ser compatível com, no mínimo, as seguintes plataformas:

1.41.12.1. Amazon Elastic Kubernetes Services (EKS);

1.41.12.2. Azure Kubernetes Services (AKS);

1.41.12.3. VMWare Tanzu;

1.41.12.4. Redhat Openshift;

1.41.12.5. Kubernetes nativo.

1.41.13. Deverá permitir a pré-filtragem do tráfego dos PODs dentro dos próprios worker nodes, evitando que tráfego desnecessário consuma os recursos de rede do worker node.

1.41.14. Deverá suportar a captura de tráfego dos PODs antes da encriptação e após a decriptação, eliminando a necessidade de posicionamento de soluções de decriptação do tipo Man-in-the-Middle (MiTM).

1.41.15. Deverá permitir a seleção de quais PODs serão monitorados baseado em atributos do próprio ambiente de conteinerização, tais como:

1.41.15.1. Namespaces;

1.41.15.2. Nomes dos serviços;

1.41.15.3. Nomes dos PODs.

1.41.16. Deverá permitir a coleta de tráfego em sistemas operacionais que não rodam sobre plataformas de virtualização suportadas através da instalação de agentes para, no mínimo, os seguintes sistemas operacionais:

1.41.16.1. Windows Server 2012 ou superior;

1.41.16.2. Windows 10 ou superior.

1.41.16.3. Distribuições Linux baseadas:

a) Redhat/CentOS/Fedora versões 7.5 ou superior;

b) Ubuntu/Debian versões 18-04 ou superior;

c) Amazon Linux versões 1 e 2.

1.41.17. Deverá permitir a pré-filtragem do tráfego nos TAPs virtuais antes de enviá-lo para as ferramentas de segurança.

1.41.18. Deverá permitir a coleta de tráfego em ambientes de nuvem, tais como AWS, Azure e GCP.

1.41.19. Deverá permitir a visualização e monitoramento da taxa de tráfego e o resumo do volume de tráfego agregado.

1.41.20. Deve implementar a funcionalidade de desencapsulamento de cabeçalhos L2GRE, VXLAN, ERSPAN e GENEVE dos pacotes de rede.

1.41.21. Deve implementar a funcionalidade de encapsulamento dos pacotes de rede com o protocolo L2GRE ou VXLAN, permitindo o envio de tráfego tunelado para as ferramentas de monitoramento, nativamente no ambiente virtual.

1.41.22. Deve implementar a funcionalidade de mascaramento de dados nos pacotes para garantir a privacidade de dados.

1.41.23. Deve implementar a funcionalidade de slicing (corte) dos pacotes, reduzindo o volume de tráfego com payloads irrelevantes.

1.41.24. Deve implementar o balanceamento de carga do tráfego para dois túneis L2GRE ou VXLAN diferentes, permitindo que sejam utilizadas ferramentas de monitoramento redundantes.

1.42. **CARACTERÍSTICAS TÉCNICAS AVANÇADAS DA SOLUÇÃO**

1.42.1. 9.3.1. Deve implementar a filtragem do tráfego de rede baseado em aplicações (camada 7).

1.42.2. 9.3.2. A funcionalidade de filtragem por aplicação deve ser capaz de reconhecer a aplicação independentemente da porta TCP ou UDP utilizada, identificando por exemplo, acessos SSH em portas fora do padrão.

1.42.3. Deve permitir que a base de aplicações seja atualizada periodicamente.

1.42.4. Deve enriquecer as informações de NetFlow com dados contextuais da camada de aplicação.

1.42.5. Deve implementar a extração de metadados do tráfego para mais de 3000 aplicações diferentes.

1.42.6. Deve extrair mais de 5000 atributos das diferentes aplicações.

1.42.7. Deve permitir o envio de metadados dados para até quatro coletores diferentes.

1.42.8. Deve implementar o envio de dados em diferentes formatos, tais como IPFIX, CEF e JSON sobre HTTPS.

1.42.9. Deve suportar a decriptação passiva (out-of-band) do tráfego TLS.

1.42.9.1. Deve implementar a captura de pacotes antes da criptografia e após a decriptação, no mínimo para os seguintes sistemas operacionais e ambientes de conteinerização:

1.42.9.2. Sistemas Linux:

a) Baseados em Debian;

b) Baseados em Redhat.

1.42.9.3. Ambientes Kubernetes:

a) AKS;

b) EKS;

c) Openshift;

d) Tanzu.

1.42.10. Deve implementar a abertura das seguintes variações de criptografias do TLS:

1.42.10.1. TLS 1.2 com PFS (Perfect Forward Secrecy);

1.42.10.2. TLS 1.3;

1.42.10.3. mTLS.

1.42.11. A funcionalidade deve ser independente de upgrades do S.O.

1.42.12. Deve implementar IPv4 e IPv6.

1.42.13. Deve implementar a biblioteca OpenSSL, no mínimo, nas seguintes versões:

1.42.14. Deve implementar a funcionalidade Packet De-Duplication (De-duplicação de Pacotes), enviando somente uma única cópia do pacote para as Ferramentas.

1.42.15. A funcionalidade de Packet De-Duplication deve implementar de-duplicação de pacotes IPv4, IPv6 e pacotes sem IP, devendo levar em consideração o Payload e os cabeçalhos ethernet.

1.42.16. A funcionalidade Packet De-Duplication deve detectar pacotes duplicados recebidos em diferentes portas ou módulos do(s) equipamento(s), inclusive se utilizado em modo Mesh/Cluster, detectando pacotes duplicados entre diferentes portas, módulos e equipamentos.

1.42.17. A funcionalidade Packet De-Duplication deve permitir habilitar ou desabilitar a inspeção de, no mínimo, os seguintes campos para avaliar se é um pacote duplicado ou não:

1.42.18. IPv4 ToS;

1.42.19. IPv6 TC;

1.42.20. Número da Sequência TCP;

1.42.21. VLAN ID.

1.42.22. Deve suportar a funcionalidade Masking (Alteração de dados), que é capaz de modificar determinadas informações contidas no tráfego de rede antes de redirecioná-lo para as Ferramentas, para atendimento de normas PCI quando necessário.

1.42.23. A funcionalidade Masking deverá ser capaz de trocar uma determinada informação como o CPF do usuário por outros caracteres (XXX.XXX.XXX-XX, por exemplo), de modo que essa informação específica seja protegida antes de ser enviada para as soluções.

- **ITEM 13 – CHASSI PARA INTERCONECTOR PASSIVO DE INTERCEPTAÇÃO DO TRÁFEGO - INTERFACES ÓPTICAS**

1.43. **CARACTERÍSTICAS TÉCNICAS**

1.43.1. Deve ser composto por um único equipamento, montável em rack 19” devendo este vir acompanhado dos devidos acessórios para tal. O equipamento deverá ser do tipo chassis/modular.

1.43.1.1. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.43.2. Deve possuir altura máxima de 1 (um) rack unit.

1.43.3. Operar em temperaturas de 0ºC a 60ºC e umidade relativa de 10% a 85%.

1.43.4. Deve ser totalmente passivo, ou seja, não é necessário nenhum tipo de alimentação elétrica, software e configuração para o seu funcionamento.

1.43.5. O chassi deverá permitir a acomodação de, no mínimo, 3 (três) dos Interconectores Passivos de Interceptação do Tráfego, seja para aqueles com interfaces SFP ou para aqueles com interfaces QSFP.

- **ITEM 14 – INTERCONECTOR PASSIVO DE INTERCEPTAÇÃO DO TRÁFEGO – INTERFACES SFP**

1.44. **CARACTERÍSTICAS TÉCNICAS**

1.44.1. Deverá ser compatível com o Chassi para Interconector Passivo de Interceptação do Tráfego.

1.44.1.1. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.44.2. O Interconector Passivo deverá possuir as seguintes características de interfaces, fibras, conectores e Split Ratio:

1.44.2.1. Possuir 2 (duas) interfaces de rede, responsável por conectar os dispositivos de rede;

1.44.2.2. Possuir 2 (duas) interfaces de monitoramento, responsável por enviar todo o tráfego TX, coletado nas interfaces de rede, em uma interface de monitoramento e todo o tráfego RX, coletado nas interfaces de rede, na outra interface de monitoramento;

1.44.3. Deverá ser fornecido com, no mínimo, 06 (seis) Interconectores Passivos ou TAPs, com a seguinte especificação: Multimodo 850nm, 50 microns, 1/10/25G com conector LC e split ratio de 50/50.

- **ITEM 15 – INTERCONECTOR PASSIVO DE INTERCEPTAÇÃO DO TRÁFEGO – INTERFACES QSFP**

1.45. **CARACTERÍSTICAS TÉCNICAS**

1.45.1. Deverá ser compatível com o Chassi para Interconector Passivo de Interceptação do Tráfego.

1.45.1.1. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.45.2. O Interconector Passivo deverá possuir as seguintes características de interfaces, fibras, conectores e Split Ratio:

1.45.2.1. Possuir 2 (duas) interfaces de rede, responsável por conectar os dispositivos de rede;

1.45.2.2. Possuir 2 (duas) interfaces de monitoramento, responsável por enviar todo o tráfego TX, coletado nas interfaces de rede, em uma interface de monitoramento e todo o tráfego RX, coletado nas interfaces de rede, na outra interface de monitoramento;

1.45.3. Deverá ser fornecido com, no mínimo, 03 (três) Interconectores Passivos ou TAPs, com a seguinte especificação: Multimodo 850nm, 50 microns, 40/100G com conector LC ou MPO e split ratio de 50/50.

- **ITEM 16 – INTERCONECTOR PASSIVO DE INTERCEPTAÇÃO DO TRÁFEGO – INTERFACES RJ-45**

1.46. **CARACTERÍSTICAS TÉCNICAS**

1.46.1. O Interconector Passivo deverá possuir os seguintes requisitos técnicos:

1.46.1.1. Deve ser composto por um único equipamento, montável em rack 19” devendo este vir acompanhado dos devidos acessórios para tal. O equipamento deverá ser do tipo chassis/modular.

1.46.1.2. Deve possuir altura máxima de 1 (um) rack unit.

1.46.1.3. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.46.2. Deverá suportar as seguintes características:

1.46.2.1. Possuir 2 (duas) interfaces de rede, responsável por conectar os dispositivos de rede;

1.46.2.2. Possuir 2 (duas) interfaces de monitoramento, responsável por enviar todo o tráfego TX, coletado nas interfaces de rede, em uma interface de monitoramento e todo o tráfego RX, coletado nas interfaces de rede, na outra interface de monitoramento;

1.46.3. Deverá ser fornecido com, no mínimo, 4 (quatro) Interconectores Passivos ou TAPs, para interceptar enlaces UTP.

- **ITEM 17 – CONCENTRADOR DE TRÁFEGO DE SEGURANÇA**

1.47. **CARACTERÍSTICAS TÉCNICAS**

1.47.1. O equipamento deverá ser fornecido com as licenças necessárias para ativação de todas as suas portas e demais funcionalidades aqui solicitadas.

1.47.1.1. Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

1.47.2. O equipamento deverá ser interligado a ao menos 1 (um) equipamentos de interceptadores de Tráfego.

1.47.3. Deverá ser compatível com transceivers SFP, SFP+, QSFP+ e QSFP28.

1.47.4. O equipamento deverá possuir, no mínimo, 1 (um) rack unit.

1.47.5. O equipamento deverá possuir, no mínimo, 2 (duas) fontes de alimentação 100-240 VAC do tipo Hot-Swap.

1.48. **CARACTERÍSTICAS DE DESEMPENHO**

1.48.1. Deverá implementar um throughput exclusivo de tráfego de processamento, no mínimo, 2 (dois) Tbps, respeitando as demais condições técnicas previstas para segurança da informação.

1.49. **CARACTERÍSTICAS FUNCIONAIS**

1.49.1. O Concentrador deverá possuir funcionalidades e hardware específicos para este propósito de agregação, regeneração, filtragem e modificação/transformação do tráfego, não sendo aceita soluções similares, como: Switches, Roteadores, Firewalls, Balanceadores, Servidores, soluções Híbridas e etc.

1.49.2. Deverá possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas de “Rede”, “Rede Inline”, “hibrida”, “circuito”, “Ferramenta” e portas de “Ferramenta Inline”.

1.49.3. Entende-se por portas de Rede, todas as portas que serão responsáveis por receber a cópia do tráfego através dos TAPs/SPANs ou Interceptadores de Tráfego.

1.49.4. Entende-se por portas de Ferramenta, todas as portas que serão responsáveis por encaminhar o tráfego, seja ele já filtrado e/ou modificado, para as ferramentas que serão conectadas ao equipamento de interceptação do tráfego.

1.49.5. Entende-se por portas de Rede Inline, todas as portas que serão responsáveis por se conectar de forma Inline a rede de produção.

1.49.6. Entende-se por portas de Ferramenta Inline, todas as portas que serão responsáveis por encaminhar o tráfego de produção, selecionado através dos filtros ou não, para as ferramentas Inline que serão conectadas ao equipamento de interceptação do tráfego.

1.50. **GERENCIAMENTO DO CONCENTRADOR**

1.50.1. O concentrador deve possuir uma interface gráfica e intuitiva com API abertas para simples customização de aplicações e integração com produtos de terceiros.

1.50.2. Deverá permitir configuração customizada baseadas nos perfis de acesso (RBAC - Role Base Access Control).

1.50.3. Deverá implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.

1.50.4. Deverá possuir suporte a MIB II.

1.50.5. Deverá implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.

1.50.6. Deverá suportar SNMP trap sobre IPv6.

1.50.7. Deverá permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface de gerenciamento.

1.50.8. Deverá permitir a gravação de log externo (syslog).

1.50.9. Deverá permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação

1.50.10. Deverá possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como estatísticas de utilização e log de eventos.

1.50.11. Deve possuir gerenciamento através de interface Web (HTTPS) e CLI.

1.50.12. Deverá implementar o protocolo NTP (Network Time Protocol).

1.50.13. Deverá implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+, RADIUS e LDAP.

1.50.14. Deve suportar IPv6 para TACACS+.

1.50.15. Deverá implementar o protocolo SSHv2 para acesso à interface de linha de comando.

1.50.16. Deverá proteger a interface de comando do equipamento através de senha.

1.51. **INTERFACES DE COMUNICAÇÃO**

1.51.1. O equipamento deverá ser fornecido com (48) portas de 1/10/25Gbps compatíveis com os padrões SFP.

1.51.2. O equipamento deverá ser fornecido com 8 (oito) portas de 40/100Gbps compatíveis com os padrões QSFP.

- **ITEM 18 – TRANSCEIVER TIPO 1 – 1 GBPS ETHERNET**

1) Deverá ser fornecido 1 (um) transceiver 1 Gbps compatível com o equipamento interceptador de tráfego.
2) Deverá ser do padrão SFP e possuir conector do tipo RJ-45.
3) Deverá ser hot-swap, permitindo a sua remoção mesmo com o equipamento ou módulo energizado.
4) Deverá ser propício para a transmissão de dados em curto alcance, permitindo atingir, no mínimo, 30 (trinta) metros de distância.
5) Deverá ser fornecido com cabos UTP, com conectores RJ-45. A metragem dos cabos será definida durante a fase de implantação da solução.
6) Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

- **ITEM 19 – TRANSCEIVER TIPO 2 – 10 GBPS ETHERNET**

1) Deverá ser fornecido 1 (um) transceiver 10 Gbps compatível com o equipamento interceptador de tráfego.
2) Deverá ser do padrão SFP+ e possuir conector do tipo LC.
3) Deverá ser hot-swap, permitindo a sua remoção mesmo com o equipamento ou módulo energizado.
4) Deverá ser propício para a transmissão de dados em curto alcance, permitindo atingir, no mínimo, 50 (cinquenta) metros de distância.
5) Deverá ser fornecido com fibras OM4 UPC, com conectores LC. A metragem das fibras será definida durante a fase de implantação da solução.
6) Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

- **ITEM 20 – TRANSCEIVER TIPO 3 – 25 GBPS ETHERNET**

1) Deverá ser fornecido 1 (um) transceiver 25 Gbps compatível com o equipamento interceptador de tráfego.
2) Deverá ser do padrão SFP28 e possuir conector do tipo LC.
3) Deverá ser hot-swap, permitindo a sua remoção mesmo com o equipamento ou módulo energizado.
4) Deverá ser propício para a transmissão de dados em curto alcance, permitindo atingir, no mínimo, 50 (cinquenta) metros de distância.
5) Deverá ser fornecido com fibras OM4 UPC, com conectores LC. A metragem das fibras será definida durante a fase de implantação da solução.
6) Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

- **ITEM 21 – TRANSCEIVER TIPO 4 – 100 GBPS ETHERNET**

1) Deverá ser fornecido 1 (um) transceiver 100 Gbps compatível com o equipamento interceptador de tráfego.
2) Deverá ser do padrão QSFP28.
3) Deverá ser hot-swap, permitindo a sua remoção mesmo com o equipamento ou módulo energizado.
4) Deverá ser propício para a transmissão de dados em curto alcance, permitindo atingir, no mínimo, 50 (cinquenta) metros de distância.
5) Deverá ser fornecido com fibras OM4 UPC. A metragem das fibras e o seu tipo de conector, LC ou MPO, serão definidos durante a fase de implantação da solução.

6) Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.

- **ITEM 22 – SERVIÇO TÉCNICO ESPECIALIZADO PARA SOLUÇÃO DE INTERCEPTAÇÃO DE TRÁFEGO**

1.52. O serviço especializado será demandado através de Ordem de Serviço (OS), prevendo o quantitativo de USTs (unidades de serviço técnico), a serem consumidos, o período de execução e a descrição dos serviços a serem executados.

1.53. A CONTRATANTE não se obriga a consumir todo o quantitativo de Unidade de Serviço Técnico (UST) de serviço especializado da CONTRATADA e pagará somente pelo quantitativo de Unidade de Serviço Técnico (UST) vinculados aos entregáveis concluídos.

1) Os serviços técnicos especializados deverão ser realizados remotamente ou presencialmente, conforme suas especificidades descritas no Catálogo de Serviços.
2) Após aceite do Ordem de Serviço por parte do CONTRATANTE, a CONTRATADA deverá executar a atividade no prazo acordado.
3) Os serviços especializados serão prestados conforme a necessidade e solicitação da CONTRATANTE mediante Ordem de Serviço, com o quantitativo de Unidade de Serviço Técnico (UST) necessários.
4) Os serviços especializados compreendem (não necessariamente nesta ordem): atividades de implantação, manutenção evolutiva, manutenção corretiva, atividades vinculadas a segurança da informação nas soluções a serem consumidas e a capacitação dos recursos humanos da CONTRATANTE.
5) Dentro de cada ordem de serviço deverá ser considerado item de planejamento (ou elaboração do plano de trabalho), que deverá conter a quantidade de USTs que suportem tal atividade. Este item deverá compreender as atividades de planejamento de execução a ser alinhado entre as partes, tendo como entregáveis: estimativas para cada item de OS, cronograma de execução e plano de trabalho.
6) Cada item da OS deverá possuir entregável(eis) claro(s), bem definido(s) e tangível(eis), de forma que a conclusão desta seja realizado apenas quando atestado a entrega do(s) serviço(s) estabelecido(s).

1.54. Conforme estabelecido no Anexo do Catálogo de Serviço.

- **LOTE III**
- **ITEM 23 – LICENCIAMENTO ELASTIC ENTERPRISE ON-PREMISE**

1.55. **CARACTERÍSTICAS GERAIS DA CONTRATAÇÃO**

1.55.1. Deverá ser fornecido licenciamento de software da solução “ELASTIC SEARCH”, na versão ENTERPRISE, ou equivalente, para sua implantação no ambiente On-premises do CONTRATANTE.

1.55.2. O licenciamento deverá ser fornecido na modalidade de subscrição, ou assinatura, não sendo admitidas versões empregadas na prestação de serviços – modalidade na qual as licenças retornam a CONTRATADA ao término do contrato.

1.55.3. A plataforma deverá permitir sua implantação no ambiente de virtualização atual do CONTRATANTE, seja ela implantada em ambiente Microsoft, Linux, VMware ou KVM. O CONTRATANTE fornecerá toda a infraestrutura base de sustentação dos servidores que deverão hospedar a plataforma.

1.55.4. Cada unidade deste licenciamento deverá fornecer, no mínimo, 64 GB (sessenta e quatro gigabytes) de memória RAM consumida ou alocada pela solução.

1.56. **PROCEDIMENTOS PARA A OPERACIONALIZAÇÃO DA SOLUÇÃO DO LOTE 03**

1.56.1. Será de responsabilidade da CONTRATADA, executar os seguintes procedimentos de instalação da solução contratada:

1.56.1.1. Apoiar na definição correta dos recursos computacionais para implantação da plataforma em ambiente on-premises da CONTRATANTE;

1.56.1.2. Instruir a CONTRATANTE quanto a arquitetura ideal dos nós da solução (master, data, ingest, coordinating e etc.).

1.56.1.3. Configurar as regras de comunicações conforme informado pela CONTRATANTE, incluindo portas, VLANs e segurança de acesso a ferramenta.

1.56.1.4. Configurações de autenticação de acesso de usuários na ferramenta.

1.56.1.5. Apoio na instalação de pacotes que compreendem os pré-requisitos da solução, como Java e demais pacotes auxiliares.

1.56.1.6. Instalação do pacote ElasticSearch.

1.56.1.7. Configuração do elasticsearch.yml, incluindo cluster name, nó master/data, seeds, heap size e caminho (path) dos dados.

1.56.1.8. Configuração de descoberta, incluindo requisições unicast de hosts.

1.56.1.9. Configuração de perfis no cluster, como node.master, node.data e etc.

1.56.1.10. Configuração de logs.

1.56.1.11. Definição de usuários, perfis e permissões.

1.56.1.12. Configuração de snapshots automáticos.

1.56.1.13. Instalação e configuração do Kibana.

1.56.1.14. Integração de Beats, incluindo Filebeat, Metricbeat e etc.

1.56.1.15. Configuração de pipelines no Logstash.

1.56.1.16. Integração de dashboards e visualizações.

1.56.2. Após o término dos procedimentos de configuração, a CONTRATADA deverá:

1.56.2.1. Executar os testes de ingestão de dados.

1.56.2.2. Executar os testes de busca e consulta na plataforma.

1.56.2.3. Executar os testes de resiliência e alta disponibilidade da solução.

1.56.2.4. CONTRATADA deverá emitir relatório As-Built de todos os procedimentos executados, incluindo diagramas lógicos e físicos.

1.56.2.5. Os procedimentos deverão ser executados presencialmente, nas mesmas dependências as quais forem instaladas as soluções, conforme determinado pela CONTRATANTE.

1.57. **REPASSE DE CONHECIMENTO NA SOLUÇÃO DO LOTE 03**

1.57.1. Após o término dos procedimentos de instalação, a CONTRATADA deverá executar repasse de conhecimento na solução implantada, sendo admitido o uso da própria solução já configurada para a execução do repasse.

1.57.2. O repasse deverá possuir duração mínima de 16 (dezesseis) horas, sendo admitida a sua divisão em 2 (dois) ou 4 (quatro) dias de repasse.

1.57.3. O serviço poderá ser executado pelo profissional mesmo profissional responsável pelos procedimentos de instalação, ou por outro profissional alocado.

1.57.4. O repasse deverá ser executado em formato on-line síncrono, de modo remoto.

1.57.5. O repasse de conhecimento deverá abordar os seguintes tópicos, minimamente:

1.57.6. Visão geral da arquitetura da solução:

1.57.6.1. Componentes da solução;

1.57.6.2. Estrutura do cluster Elastic Search;

1.57.6.3. Integração com outros componentes da solução.

1.57.7. Acesso e gerenciamento:

1.57.7.1. Interface de gerenciamento e configuração da solução;

1.57.7.2. Painel de controle da solução;

1.57.7.3. Procedimentos de backup das configurações;

1.57.7.4. Configuração de serviços internos de rede da solução.

1.57.8. Administração:

1.57.8.1. Criação de índices;

1.57.8.2. Políticas de ILM;

1.57.8.3. Ajustes de mapeamentos de dados.

1.57.9. Operação:

1.57.9.1. Depuração e troubleshooting;

1.57.9.2. Abertura de chamados;

1.57.9.3. Gerenciamento de licenças.

1.58. **CARACTERÍSTICAS TÉCNICAS DA PLATAFORMA**

1.59. A solução deverá ter a capacidade para ampliar o poder de processamento tanto por meio da escalabilidade horizontal (mais máquinas) como da escalabilidade vertical (melhoria de características de hardware);

1.60. A solução deverá ter a capacidade de manter cópias redundantes dos dados e proporcionar uma recuperação rápida em caso de falha do sistema ou desastre;

1.61. A solução deverá executar a busca assertiva e o acesso rápido aos dados procurados;

1.62. A solução deverá executar a busca ampla e irrestrita de textos, dados, termos, informações ou outras demandas, em qualquer solução, sistema, aplicação ou plataforma, através de acesso a todo e qualquer repositório de dados, sejam documentos, logs, banco de dados, registros, códigos-fonte ou qualquer outro arquivo com vista à geração de conhecimento de forma segura e segmentada;

1.63. A busca, executada pela ferramenta, deverá ser capaz de ser realizada nos seguintes tipos: full-text, autocomplete, spell, checker e multifield;

1.64. A solução deverá possuir controle de acesso baseado em atributos;

1.65. A solução deverá permitir seu crescimento horizontal, garantindo alta disponibilidade, sem que haja limitação relativa ao volume de dados a serem ingeridos;

1.66. A solução deverá deter da possibilidade de distribuição de dados em diferentes tipos de discos (rápidos/lentos) de acordo com a criticidade estabelecida;

1.67. A solução deverá deter da possibilidade de implantação em hardware físico e máquinas virtuais (ambiente on-premises);

1.68. A solução deverá permitir a provisão e o gerenciamento de vários clusters de maneira centralizada;

1.69. A solução deverá possuir gerenciamento de usuários e funções;

1.70. A solução deverá incluir a utilização otimizada de recursos e o isolamento baseado no uso de containers;

1.71. A oferta deverá incluir suporte homologado e apoio técnico especializado do fabricante;

1.72. A solução deve ser capaz de indexar e realizar buscas tanto nos ambientes on-premises quanto em nuvem, conforme a melhor arquitetura de consumo da solução pelo CONTRATANTE.

- **ITEM 24 – SERVIÇO TÉCNICO ESPECIALIZADO PARA O LICENCIAMENTO ELASTIC ENTERPRISE ON-PREMISE**

1.73. O serviço especializado será demandado através de Ordem de Serviço (OS), prevendo o quantitativo de USTs (unidades de serviço técnico), a serem consumidos, o período de execução e a descrição dos serviços a serem executados.

1.74. A CONTRATANTE não se obriga a consumir todo o quantitativo de Unidade de Serviço Técnico (UST) de serviço especializado da CONTRATADA e pagará somente pelo quantitativo de Unidade de Serviço Técnico (UST) vinculados aos entregáveis concluídos.

1) Os serviços técnicos especializados deverão ser realizados remotamente ou presencialmente, conforme suas especificidades descritas no Catálogo de Serviços.
2) Após aceite do Ordem de Serviço por parte do CONTRATANTE, a CONTRATADA deverá executar a atividade no prazo acordado.
3) Os serviços especializados serão prestados conforme a necessidade e solicitação da CONTRATANTE mediante Ordem de Serviço, com o quantitativo de Unidade de Serviço Técnico (UST) necessários.
4) Os serviços especializados compreendem (não necessariamente nesta ordem): atividades de implantação, manutenção evolutiva, manutenção corretiva, segurança da informação e auditoria nas soluções a serem consumidas, personalização da camada de negócios e capacitação dos recursos humanos da CONTRATANTE.
5) Dentro de cada ordem de serviço deverá ser considerado item de planejamento (ou elaboração do plano de trabalho), que deverá conter a quantidade de USTs que suportem tal atividade. Este item deverá compreender as atividades de planejamento de execução a ser alinhado entre as partes, tendo como entregáveis: estimativas para cada item de OS, cronograma de execução e plano de trabalho.
6) Cada item da OS deverá possuir entregável(eis) claro(s), bem definido(s) e tangível(eis), de forma que a conclusão desta seja realizado apenas quando atestado a entrega do(s) serviço(s) estabelecido(s).

1.75. Conforme estabelecido no Anexo do Catálogo de Serviço.

1.76. **Necessidades de Adequações no Ambiente / Implantação**

1.76.1. A implantação da solução requer uma avaliação da CONTRATANTE quanto à possível ncessidade de adequação da infraestrutura de TI existente. As principais áreas que precisam ser revisadas e, possivelmente, ajustadas antes da contratação são:

1.76.2. Fonte de Energia e Climatização: A adequação da infraestrutura física do data center é essencial para suportar os novos equipamentos. O aumento da densidade computacional, proporcionado pela appliances da solução, pode demandar revisões por parte da CONTRATANTE na capacidade de fornecimento de energia e no sistema de refrigeração, para evitar sobrecargas e garantir o resfriamento adequado dos equipamentos.

1.76.3. Capacitação da Equipe: A adoção de novas tecnologias geralmente demanda uma curva de aprendizado para a equipe de TI. Portanto, um plano de capacitação deve ser desenvolvido, incluindo treinamentos formais e workshops para que os profissionais estejam preparados para administrar e operar o ambiente com eficiência.

1.76.4. Infraestrutura: Pode haver necessidade de disponibilização de conexões físicas e lógicas destinadas ao equipamento a ser instalado, bem como pontos de rede no switch-core para o appliance a ser instalado.

1.76.5. Conclusão: A adequação do ambiente é um passo crítico para o sucesso da implementação da solução. A CONTRATANTE deve proceder, antes da contratação, com uma análise detalhada e realizr, se necessário, ajustes nas áreas de infraestrutura física e segurança para garantir que a nova solução seja plenamente aproveitada, proporcionando maior performance, resiliência e facilidade de gestão.

1.77. **REUNIÃO DE KICK-OFF**

1.77.1. A CONTRATADA deve realizar, antes do início da implantação da solução, uma reunião inicial de projeto (kick-off) com a CONTRATANTE.

1.77.2. A CONTRATANTE deverá acionar as suas áreas que serão responsáveis pela Segurança da Informação, Infraestrutura, Gestão e Fiscalização do Contrato, para em conjunto com a CONTRATADA para definirem o local de implantação, preparação do ambiente, instalação e configuração da solução.

1.77.3. Após a reunião de kick-off deve ser produzida uma ata e assinada por todos os participantes da CONTRATADA e da CONTRATANTE presentes, contemplando o planejamento, escopo, cronograma, discriminação dos produtos entregáveis, dimensionamento da infraestrutura tecnológica necessária, discriminação da EQUIPE do projeto com perfis e quantitativos mínimos, relatório de controle e tratamento de riscos do projeto e demais artefatos que se façam necessários no entendimento da Contratada.

1.77.4. Na reunião inicial, serão abordados alguns pontos e informações citadas a seguir, mas não limitando-se a:

1.77.5. Apresentação das equipes envolvidas, com definição dos responsáveis técnicos e gerenciais de ambas as partes;

1.77.6. Validação do escopo detalhado dos produtos e serviços contratados, com ênfase nas etapas de instalação, configuração, suporte técnico e treinamentos;

1.77.7. Definição e validação do cronograma de execução, com marcos de entregas, prazos intermediários e critérios para aceite de cada fase;

1.77.8. Estabelecimento dos canais formais de comunicação e reporte, assim como dos instrumentos de acompanhamento e controle da execução contratual (relatórios, reuniões periódicas, ferramentas de gestão, etc.);

1.77.9. Levantamento e verificação de pré-requisitos técnicos e operacionais para o início da execução, incluindo:

a) Disponibilidade e configuração dos ambientes (produção e testes);
b) Necessidade de provisionamento de acessos, credenciais e perfis de usuários;
c) Infraestrutura mínima necessária (rede, banco de dados, servidores, etc.);
d) Integrações com sistemas legados eventualmente envolvidos;
e) Apoio necessário por parte da equipe interna da contratante; e
f) Dinâmica de capacitação;

1.78. **Plano de Trabalho**

1.78.1. Plano de Trabalho é o documento que detalha como os serviços contratados serão executados.

1.78.2. A CONTRATADA deverá elaborar o Plano de Trabalho abordando alguns pontos e informações citadas a seguir, mas não limitando-se a:

a) Nome do Serviço;
b) Escopo;
c) Descrição Detalhada;
d) Atividades e Entregáveis Previstos;
e) Esforço Estimado;
f) Complexidade da Demanda;
g) Definição das Responsabilidades;
h) Cronograma;
i) Perfis Profissionais Envolvidos; e

j) Quantidade e Valor de Unidade de Serviço Técnico (UST), bem como prazo de execução.

1.78.3. O pagamento estará condicionado à prestação do serviço, que deverá ser precedido de um Plano de trabalho para abertura de Ordem de Serviço (OS).

1.78.4. Para a execução de uma demanda poderá ser registrada mais de uma OS, devendo cada uma representar um conjunto inter-relacionado de funcionalidades ou artefatos que contemplem e delimitem uma fase ou iteração.

1.78.5. Qualquer alteração nas definições descritas na OS deverá gerar uma nova OS de solicitação de mudança, que será anexada a OS original.

1.78.6. Reedições do Plano de Trabalho com recebimento definitivo, desde que demandadas pelo CONTRATANTE e que sejam derivadas de mudança de escopo. O processo de execução do serviço poderá ser alterado a qualquer momento, em comum acordo entre CONTRATANTE e CONTRATADA.

1.78.7. A execução do objeto será iniciada a partir da emissão da Ordem de Serviço, o qual autoriza a licitante vencedora a seguir e cumprir o cronograma de atividades.

Rio de Janeiro, na data da assinatura eletrônica.

Documento assinado eletronicamente por **Rodolfo Targino de Araujo**, **Assistente**, em 23/03/2026, às 14:14, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Luís Cláudio Marinho Coelho**, **Gerente**, em 23/03/2026, às 14:26, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor-Chefe**, em 23/03/2026, às 14:27, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Roberto Charles Vilas**, **Diretor**, em 23/03/2026, às 14:28, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 23/03/2026, às 14:33, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **128113020** e o código CRC **F8644F31**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro
Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro
Vice Presidência de Tecnologia

ANEXO II

CATÁLOGO DE SERVIÇOS

1. CATÁLOGO DE SERVIÇOS REFERENTES À UNIDADE DE SERVIÇO TÉCNICO – UST

1.1. O catálogo de serviços estabelece as atividades dentro de cada fase da Solução de interceptação de tráfego, monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, com Instalação da Solução, incluindo hardware, software e demais componentes, bem como serviços de treinamento e garantia com manutenção do fabricante por 36 (trinta e seis) meses. As Ordens de Serviço para execução dos projetos serão realizadas a partir do consumo de UST dos itens do catálogo.

1.2. Os serviços técnicos especializados relativos aos sistemas e suporte a soluções de automação com atendimento remoto e on-site (no local), serão realizados sob demanda, a partir de um conjunto de atividades estabelecido no Catálogo de Serviços, aqui apresentado, em consonância com as etapas previstas no planejamento de execução dos projetos, e estabelece uma sequência de atividades que podem ser aplicadas no desenvolvimento de cada projeto, bem como, da complexidade típica esperada na realização das atividades preconizadas.

1.3. Os serviços técnicos especializados terão como unidade de medida a “unidade de serviço técnico” (UST) e serão requisitados, sob demanda, por meio de ordem de serviço.

1.4. O modelo de quantificação por UST é baseado na quantificação detalhada de cada esforço de trabalho realizado para obtenção dos serviços necessários no escopo deste Estudo Técnico Preliminar.

1.5. A fim de uniformizar o entendimento sobre os termos utilizados, seguem algumas definições:

- Unidade de Serviço Técnico – UST: métrica utilizada para aferir o custo de cada atividade a ser desempenhada;
- Custo em UST – representa o custo de cada atividade, considerando o tempo de duração em UST e o peso de cada UST; e
- Duração em UST – Tempo de duração para execução de cada atividade, considerando que uma UST tem a duração de 60 minutos.

1.6. A tabela a seguir apresenta o quantitativo de UST para cada hora de trabalho dados os respectivos graus de complexidade:

COMPLEXIDADE DO SERVIÇO TÉCNICO	
Complexidade	**Fator de Ajuste**
Baixa	1,00
Média	1,25
Alta	1,50

Lote I - Item 2 - Do Quantitativo de Serviços e Memória de cálculo - UST

Atividade	Complexidade (Baixa, Média ou Alta)	Tipo de Execução (Remota ou Presencial)	Duração do Serviço (horas)	Validação dos Serviços Executados (horas)	Documentação dos Serviços Executados (horas)	Total Estimado de Horas	UST ajustada conforme a complexidade	Quantidade em 3 anos	Estimado de UST's
ATIVIDADES DE ARQUITETURA E PROJETO									

Levantamento de requisitos de tráfego e proteção de rede	MÉDIA	PRESENCIAL	18	6	8	32	40	1	40
Levantamento de requisitos de proteção automatizada	MÉDIA	PRESENCIAL	24	3	8	35	44	1	44
Mapeamento de topologia de rede e pontos de coleta	ALTA	PRESENCIAL	12	8	24	44	66	1	66
Dimensionamento de capacidade de throughput	MÉDIA	PRESENCIAL	26	6	12	44	55	3	165
Configuração física no rack (energia, cabeamento, rede de gestão)	MÉDIA	PRESENCIAL	24	6	12	42	53	1	53
Configuração da Solução de Gerenciamento Centralizado	MÉDIA	REMOTO	6	1	2	9	11	1	11
Definição de VLAN tags para análise de tráfego de rede	ALTA	PRESENCIAL	15	4	8	27	41	2	81
Configuração de tráfego e origem do tráfego	MÉDIA	PRESENCIAL	18	6	10	34	43	3	128
Integração com ferramentas de cibersegurança (Firewall, IDS/IPS, SIEM)	ALTA	REMOTO	20	8	18	46	69	3	207
Criação de documentação sobre a arquitetura do ambiente	BAIXA	REMOTO	12	0	0	12	12	1	12
Configuração de Interfaces, VLANs e Roteamento	MÉDIA	PRESENCIAL	16	2	3	21	26	3	79
Ativação IDS/IPS e Perfis de Inspeção	ALTA	PRESENCIAL	20	8	8	36	54	3	162
Configuração de integração entre os componentes	MÉDIA	PRESENCIAL	12	4	6	22	28	3	83
Descoberta e cadastros de assets na rede	MÉDIA	REMOTO	8	1	2	11	14	3	41
Configuração de Syslog para envio à terceiros	MÉDIA	REMOTO	6	1	2	9	11	3	34
Configuração de Syslog para recebimento de terceiros	MÉDIA	REMOTO	6	1	2	9	11	3	34
ATIVIDADES DE MANUTENÇÃO CONTÍNUA									

Configuração de Perfils de Inspeção	MÉDIA	REMOTO	8	6	10	24	30	12	360
Atualização de Firmware / Assinaturas	MÉDIA	REMOTO	8	1	2	11	14	6	83
Ajustes periódicos nas regras de detecção tráfego	MÉDIA	REMOTO	10	4	6	20	25	18	450
Inclusão ou remoção de configuração de espelhamento	MÉDIA	REMOTO	8	2	4	14	18	6	105
Inclusão ou remoção de configuração de resposta via XDR com terceiros	MÉDIA	REMOTO	10	6	19	35	44	6	264
Inclusão ou remoção de configuração de resposta via IPS	MÉDIA	REMOTO	12	4	5	21	26	6	156
Geração de relatórios de detecções e ameaças	MÉDIA	REMOTO	8	6	17	31	39	12	468
Revisão de integrações com sistemas terceiros	ALTA	PRESENCIAL	24	8	24	56	84	6	504
Treinamentos de reciclagem para operação por Aluno - 16 horas divididos em 4 dias de modo remoto e síncrono	MÉDIA	REMOTO	24	0	0	24	30	2	60
Análise e revisão de regras de detecção	MÉDIA	REMOTO	10	6	12	28	35	6	210
Análise e revisão de regras de resposta	MÉDIA	REMOTO	8	6	12	26	33	6	198
Criação de regras de detecção e correlação customizadas	ALTA	REMOTO	24	12	24	60	90	3	270
Criação de regras (playbooks) customizadas para respostas automatizadas	ALTA	REMOTO	24	12	24	60	90	6	540
ATIVIDADES ESPECIALIZADAS									
Consultoria de arquitetura de visibilidade, incluindo possíveis melhorias e health-check da solução	ALTA	PRESENCIAL	24	8	24	56	84	3	252
Desenho de topologia de site	MÉDIA	PRESENCIAL	12	0	18	30	38	2	75
Apoio em provas de conceito para o teste de funcionalidades na solução implantada	MÉDIA	REMOTO	12	6	10	28	35	3	105

Revisão de melhores práticas de configuração	MÉDIA	REMOTO	10	6	6	22	28	3	83
Desenvolvimento de scripts e perfils de automação	ALTA	REMOTO	16	2	3	21	32	6	192
Apoio a construção de laboratório de testes na solução implantada	MÉDIA	REMOTO	12	6	10	28	35	3	105
Suporte em auditoria forenses de incidentes de segurança	ALTA	REMOTO	70	0	10	80	120	3	360
TOTAL									**6.080**

Lote II - Item 22 - Do Quantitativo de Serviços e Memória de cálculo - UST

CATÁLOGO DE USTS (1 UST = 1 HORA)									
Atividade	**Complexidade (Baixa, Média ou Alta)**	**Tipo de Execução (Remoto ou Presencial)**	**Duração do Serviço (horas)**	**Validação dos Seviços Executados (horas)**	**Documentação dos Serviços Executado (Horas)**	**Total Estimado de Horas**	**UST AJUSTADA CONFORME A COMPLEXIDADE**	**Quantidade em 3 anos**	**ESTIMADO DE USTs**
ATIVIDADES DE ARQUITETURA E PROJETO									
Levantamento de requisitos de tráfego	MEDIA	PRESENCIAL	24	4	24	52	65	2	130
Mapeamento de topologia de rede e pontos de coleta (TAP/SPAN)	ALTA	PRESENCIAL	36	6	12	54	81	2	108
Definição de arquitetura de Rede (appliances, módulos, links)	MEDIA	REMOTO	12	6	8	26	32	2	52
Dimensionamento de capacidade de throughput	MEDIA	REMOTO	16	6	8	30	37	2	60
Configuração física no rack (energia, cabeamento, rede de gestão)	MEDIA	PRESENCIAL	12	2	8	22	27	2	44
Inicialização de chassi e módulos de linha	ALTA	PRESENCIAL	6	6	3	15	22	2	30
Configuração da Solução de	ALTA	PRESENCIAL	8	1	8	17	25	2	34

Gerenciamento Centralizado									
Definição de VLAN tags para controle de tráfego	ALTA	PRESENCIAL	5	1	3	9	13	2	18
Definição de filtros de tráfego	MEDIA	REMOTO	6	1	3	10	12	2	20
Configuração de agregação de portas (Port Aggregation Groups)	ALTA	REMOTO	6	1	3	10	15	2	20
Configuração de filtros de exclusão (block lists)	ALTA	REMOTO	6	1	3	10	15	2	20
Ajustes de política de Desduplicação	MEDIA	REMOTO	6	1	3	10	12	2	20
Configuração de packet slicing (redução de payload)	ALTA	REMOTO	6	1	3	10	15	2	20
Ativação de NetFlow ou IPFIX para geração de metadados	MEDIA	REMOTO	4	1	3	8	10	2	16
Configuração Lógica de SSL/TLS Decryption	MEDIA	REMOTO	4	1	3	8	10	2	16
Definição de regras de Balanceamento de Carga	MEDIA	REMOTO	4	1	3	8	10	2	16
Configuração de tunelamento para tráfego encapsulado	ALTA	REMOTO	8	1	3	12	18	2	24
Configuração de Inline Bypass (proteção de falha em equipamentos inline)	ALTA	PRESENCIAL	4	1	3	8	12	2	16
Integração com sistemas de monitoramento NMS	MEDIA	REMOTO	4	1	3	8	10	2	16
Integração com ferramentas de cibersegurança	ALTA	REMOTO	48	1	3	52	78	2	104

(Firewall, IDS/IPS, SIEM, EDR ou NDR)									
Testes de desempenho do link monitorado	MEDIA	REMOTO	6	1	3	10	12	2	20
Testes de failover / alta disponibilidade	ALTA	PRESENCIAL	8	1	3	12	18	2	24
Validação de visibilidade ponta a ponta	MEDIA	REMOTO	12	1	3	16	20	2	32
Criação de documentação sobre a arquitetura do ambiente	BAIXA	REMOTO	48	0	0	48	48	2	96
ATIVIDADES DE MANUTENÇÃO CONTÍNUA									
Monitoramento do estado de portas e links	BAIXA	REMOTO	4	1	3	8	8	2	16
Monitoramento de utilização de CPU/memória dos appliances	BAIXA	REMOTO	4	1	3	8	8	2	16
Ajustes periódicos nos filtros de tráfego	MEDIA	REMOTO	6	1	3	10	12	2	20
Inclusão ou remoção de destinos de análise	MEDIA	REMOTO	4	1	3	8	10	2	16
Ajustes de balanceamento de tráfego	MEDIA	REMOTO	4	1	3	8	10	2	16
Atualização de firmware dos appliances	ALTA	REMOTO	4	1	3	8	12	2	16
Aplicação de patches de segurança	ALTA	REMOTO	2	1	3	6	9	2	12
Validação de regras de desduplicação	MEDIA	REMOTO	2	1	3	6	7	2	12
Revisão de políticas de movimentação ou reencaminhamento do tráfego	MEDIA	REMOTO	3	1	3	7	8	2	14

Análise de logs do gerenciamento centralizado ou dos appliances	MEDIA	REMOTO	4	1	3	8	10	2	16
Criação de rotinas de backups de configuração	MEDIA	REMOTO	3	1	3	7	8	2	14
Análise do consumo de licenças	BAIXA	REMOTO	2	1	3	6	6	2	12
Auditoria de filtros e políticas	BAIXA	REMOTO	6	1	3	10	10	2	20
Geração de relatórios de tráfego visível	MEDIA	REMOTO	4	1	3	8	10	2	16
Investigação de incidentes quanto a camada de tráfego interceptado	MEDIA	REMOTO	8	1	3	12	15	2	24
Troubleshooting de falhas de visibilidade	MEDIA	REMOTO	6	1	3	10	12	2	20
Reavaliação do dimensionamento aplicado frente ao crescimento de tráfego	MEDIA	REMOTO	12	1	3	16	20	2	32
Testes de contingência programados	ALTA	REMOTO	24	1	3	28	42	2	56
Revisão de integrações com ferramentas externas	MEDIA	REMOTO	6	1	3	10	12	2	20
Treinamentos de reciclagem para operação por Aluno - 16 horas divididos em 4 dias de modo remoto e síncrono	MEDIA	REMOTO	16	0	0	16	20	2	32
Apoio na coleta de dados para ampliação do dimensionamento presente	MEDIA	REMOTO	4	1	3	8	10	2	16
Otimização de regras para reduzir	MEDIA	REMOTO	4	1	3	8	10	2	16

latência									
Validação de atualização de sistemas terceiros integrados	MEDIA	REMOTO	3	1	3	7	8	2	14
Criação de mecanismos que auxiliam o controle de mudanças no ambiente	MEDIA	REMOTO	4	1	3	8	10	2	16
ATIVIDADES ESPECIALIZADAS									
Consultoria de arquitetura de visibilidade, incluindo possíveis melhorias e health-check da solução	MEDIA	REMOTO	24	0	3	27	33	6	162
Desenho de topologia multi-site	ALTA	REMOTO	30	0	3	33	49	2	66
Apoio em provas de conceito para o teste de funcionalidades na solução implantada	ALTA	REMOTO	12	2	3	17	25	2	34
Revisão de melhores práticas de configuração	MEDIA	REMOTO	8	1	3	12	15	6	72
Integração customizada via API	ALTA	REMOTO	24	1	3	28	42	2	56
Desenvolvimento de scripts de automação	ALTA	REMOTO	36	1	3	40	60	2	80
Apoio em projetos de expansão de rede	MEDIA	REMOTO	30	1	3	34	42	6	204
Assessoria em estratégias Zero Trust	ALTA	REMOTO	30	1	3	34	51	2	68

Elaboração de relatórios executivos (C-level) com dados de tráfego e visibilidade	ALTA	REMOTO	48	0	0	48	72	2	96
Consultoria para segmentação de tráfego sensível	ALTA	REMOTO	40	2	3	45	67	2	90
Suporte em auditorias forenses de incidentes de segurança	ALTA	REMOTO	60	2	3	65	97	2	130
Configuração e teste de de descriptografia do tráfego	ALTA	REMOTO	36	2	3	41	61	2	82
Monitoramento proativo gerenciado - Mensal (NOC)	MEDIA	REMOTO	12	0	0	12	15	36	432
Configuração de dashboards customizados	ALTA	REMOTO	40	1	3	44	66	2	88
Definição de KPIs de visibilidade de rede	MEDIA	REMOTO	30	1	3	34	42	2	68
Configuração e gerenciamento de TAPs óticos de alta densidade	ALTA	REMOTO	12	2	3	17	25	2	34
Apoio à construção de laboratório de testes na Solução Implantada	MEDIA	REMOTO	24	2	3	29	36	2	58
TOTAL									**3.238**

Lote III - Item 24 - Do Quantitativo de Serviços e Memória de cálculo - UST

Atividade	Complexidade (Baixa, Média ou Alta)	Tipo de Execução (Remoto ou Presencial)	Duração do Serviço (horas)	Validação dos Seviços Executados (horas)	Documentação dos Serviços Executado (Horas)	Total Estimado de Horas	UST AJUSTADA CONFORME A COMPLEXIDADE	QUANTIDADE	TOTAL ESTIMADO
ATIVIDADES DE ARQUITETURA E PROJETO									

Levantamento de requisitos de armazenamento e retenção de dados	BAIXA	REMOTO	6	6	6	18	18	2	36
Dimensionamento de nós (master, data, ingest, coordinating)	ALTA	REMOTO	8	7	6	21	31	2	62
Planejamento de capacidade de CPU, memória e I/O	MEDIA	REMOTO	6	2	4	12	15	2	30
Planejamento de rede (interfaces, VLANs, roteamento)	ALTA	REMOTO	10	7	6	23	34	2	68
Instalação do sistema operacional nos servidores	MEDIA	REMOTO	4	4	3	11	13	2	26
Instalação do Elasticsearch e componentes (Kibana, Logstash, Beats)	ALTA	REMOTO	16	7	6	29	43	2	86
Configuração de cluster (endpoints, seeds, discovery)	MEDIA	REMOTO	6	5	6	17	21	2	42
Definição de política de shards e réplicas	ALTA	REMOTO	10	3	6	19	28	2	56
Configuração de índices padrão	ALTA	REMOTO	10	3	6	19	28	2	56
Configuração de templates de índice	ALTA	REMOTO	10	3	6	19	28	2	56
Definição de políticas de index lifecycle management (ILM)	ALTA	REMOTO	10	3	6	19	28	2	56
Configuração de snapshot e backup	MEDIA	REMOTO	6	3	4	13	16	2	32
Configuração de autenticação (LDAP, SAML, Active Directory)	ALTA	REMOTO	8	6	4	18	27	2	54
Integração com sistemas de monitoramento	ALTA	REMOTO	16	10	8	34	51	2	102

externo (Zabbix, Prometheus, etc.)									
Ativação de TLS/SSL nos nós do cluster	MEDIA	REMOTO	8	8	6	22	27	2	54
Configuração de firewall e regras de segurança	MEDIA	REMOTO	8	5	6	19	23	2	46
Configuração de roles e permissões (RBAC)	MEDIA	REMOTO	6	6	4	16	20	2	40
Criação de dashboards iniciais no Kibana	ALTA	REMOTO	24	14	12	50	75	2	150
Testes de carga e stress do cluster	ALTA	REMOTO	48	40	36	124	186	2	372
Testes de failover e resiliência	ALTA	REMOTO	24	12	8	44	66	2	132
Documentação da arquitetura final	BAIXA	REMOTO	60	8	0	68	68	2	136
Treinamento introdutório para operação - 16h remoto, por Aluno	MEDIA	REMOTO	24	0	0	24	30	6	180
ATIVIDADES DE MANUTENÇÃO CONTÍNUA									
Monitoramento de uso de disco nos nós	MEDIA	REMOTO	15	1	1	17	21	3	63
Monitoramento de índices (tamanho, crescimento, quantidade de shards)	MEDIA	REMOTO	15	1	1	17	21	3	63
Ajustes de index lifecycle policies	MEDIA	REMOTO	4	1	1	6	7	3	21
Rotina de rotação de índices	BAIXA	REMOTO	4	1	1	6	6	3	18
Atualização de pacotes e plugins do Elastic	ALTA	REMOTO	6	1	1	8	12	3	36
Aplicação de patches de segurança	ALTA	REMOTO	6	1	1	8	12	3	36
Ajustes de configuração de heap da JVM	MEDIA	REMOTO	4	1	1	6	7	3	21
Monitoramento de consumo de	BAIXA	REMOTO	15	1	1	17	17	3	51

CPU/memória									
Monitoramento de filas do Logstash	BAIXA	REMOTO	15	1	1	17	17	3	51
Ajustes de ingest pipelines	ALTA	REMOTO	8	1	1	10	15	3	45
Gerenciamento de snapshots e backups periódicos	MEDIA	REMOTO	15	1	1	17	21	3	63
Validação de integridade dos dados restaurados	ALTA	REMOTO	8	1	1	10	15	3	45
Análise de performance de queries	ALTA	REMOTO	8	1	1	10	15	3	45
Troubleshooting de falhas de cluster	ALTA	REMOTO	16	1	1	18	27	3	81
Rebalanceamento de shards	ALTA	REMOTO	8	1	1	10	15	3	45
Testes de recuperação de desastres (DR)	ALTA	REMOTO	12	1	1	14	21	3	63
Auditoria de permissões e roles periodicamente	MEDIA	REMOTO	4	1	1	6	7	3	21
Validação de integrações (ex.: SIEM, NDR ou outras plataformas)	MEDIA	REMOTO	4	1	1	6	7	3	21
Revisão de dashboards e relatórios no Kibana	ALTA	REMOTO	16	1	1	18	27	3	81
Otimização de mapeamentos de índices	ALTA	REMOTO	4	1	1	6	9	3	27
Apoio a investigações em logs	BAIXA	REMOTO	3	1	1	5	5	3	15
Coleta de métricas para redimensionamento do ambiente	MEDIA	REMOTO	6	1	1	8	10	3	30
Testes de alta disponibilidade em caso de falha de link/rede	ALTA	REMOTO	8	1	1	10	15	3	45
ATIVIDADES ESPECIALIZADAS									

Consultoria de arquitetura da solução Elastic, incluindo possíveis melhorias e health-check da solução	MEDIA	REMOTO	12	1	1	14	17	3	51
Consultoria em pipelines de ingest complexos (Logstash, Beats, ingest pipelines)	ALTA	REMOTO	6	1	1	8	12	3	36
Integração do Elastic Stack com SIEMs de terceiros	ALTA	REMOTO	24	1	1	26	39	2	78
Configuração de monitoramento avançado (Metricbeat, APM)	ALTA	REMOTO	16	1	1	18	27	3	81
Desenho de alta disponibilidade e disaster recovery	ALTA	REMOTO	36	1	1	38	57	2	114
Apoio a testes de stress e desempenho	MEDIA	REMOTO	40	1	1	42	52	6	312
Apoio a migração de dados legados	ALTA	REMOTO	48	1	1	50	75	3	225
Desenvolvimento de dashboards customizados no Kibana	ALTA	REMOTO	12	1	1	14	21	6	126
Integração com ferramentas de automação (Ansible, Puppet, Chef)	ALTA	REMOTO	48	1	1	50	75	3	225
Desenvolvimento de scripts de manutenção automatizada	ALTA	REMOTO	24	1	1	26	39	3	117
Apoio a projetos de observabilidade fim-a-fim (logs, métricas, traces)	MEDIA	REMOTO	12	1	1	14	17	6	102
Monitoramento proativo gerenciado - Mensal (NOC)	MEDIA	REMOTO	15	1	1	17	21	36	756
TOTAL DE USTS									**5.082**

1.7. **SOLICITAÇÃO DO SERVIÇO ESPECIALIZADO**

1.7.1. A solicitação do serviço especializado ocorrerá sob demanda, mediante abertura de ordem de serviço (OS) em conformidade com as necessidades da CONTRATANTE ao longo da execução do contrato.

1.7.2. O modelo de prestação dos serviços é representado, pelo fluxo da OS, definido na tabela seguinte:

PASSO	RESPONSÁVEL	AÇÃO
1	CONTRATANTE	Registrar uma minuta de OS descrevendo a demanda a ser atendida
2	CONTRATADA	Analisa a minuta e apresenta proposta de execução com a previsão de itens de catálogo, estimativas de UST e de prazos de início dos serviços.
3	CONTRATANTE	Avalia proposta e autoriza a execução da OS
4	CONTRATADA	Na data prevista de início: Aloca os recursos necessários e inicia a execução.
5	CONTRATADA	Entrega os produtos da OS para avaliação
6	CONTRATANTE	Faz recebimento provisório da OS
7	CONTRATANTE	Avalia cada produto, registrando os defeitos encontrados.
8	CONTRATADA	Corrige os defeitos e submete produtos a nova avaliação (retorna ao passo 7)
9	CONTRATADA	Apresenta a contagem detalhada das UST
10	CONTRATANTE	Avalia e aprova a contagem detalhada.
11	CONTRATANTE	Quando todos os produtos e a contagem detalhada forem aprovados, faz o recebimento definitivo e encerra a OS

Rio de Janeiro, na data da assinatura eletrônica.

Documento assinado eletronicamente por **Rodolfo Targino de Araujo**, **Assistente**, em 23/03/2026, às 14:14, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Luís Cláudio Marinho Coelho**, **Gerente**, em 23/03/2026, às 14:26, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor-Chefe**, em 23/03/2026, às 14:27, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Roberto Charles Vilas**, **Diretor**, em 23/03/2026, às 14:28, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 23/03/2026, às 14:33, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

ANEXO III - PROVA DE CONCEITO I

1. INTRODUÇÃO

1.1. A prova de conceito consistirá na apresentação do funcionamento dos Serviços de Fábrica de Teste, Qualidade e Métricas.

1.1.1. O referido LICITANTE será convocado no prazo de até 10 (dez) dias úteis, a contar da aprovação da sua documentação de habilitação, para uma reunião preparatória (que poderá ocorrer em plataforma virtual), onde serão definidas as providências necessárias ao ambiente de teste da POC. Nessa reunião o LICITANTE deverá informar os requisitos necessários para a instalação do ambiente de teste a serem disponibilizados pelo PRODERJ conforme entendimento durante a reunião. Entende-se por "requisitos necessários":

a) Disponibilização de máquinas virtuais e/ou estações de trabalho, projetor e link de internet;

b) Criação de VLAN's e/ou disponibilização de endereços IP e entrada de DNS;

c) Criação de servidores de aplicação web;

d) Criação de usuários no AD e/ou modificações de regras de firewall, IPS, etc;

e) Caso seja aplicável, a disponibilização de periféricos, tais como: cabos, switches e outros componentes semelhantes não mencionados.

1.1.2. Nesta reunião preparatória, o LICITANTE deverá, sob pena de desclassificação, entregar os documentos da(s) solução(ões) que permitam comprovar o atendimento aos requisitos técnicos constantes do Anexo I deste documento, apresentando no mínimo:

a) ID do requisito;

b) Descrição do requisito;

c) Nome do produto ofertado (modelo, marca e fabricante);

d) Nome do documento de referência onde é possível verificar evidência do atendimento do requisito;

e) Página do documento referência onde é possível verificar evidência do atendimento do requisito;

f) Outras informações necessárias.

1.1.3. O LICITANTE será responsável por todos os custos inerentes à realização da prova de conceito, tais como despesas com viagens, estadas, equipe técnica, equipamentos, assim como, pela geração dos dados simulados que deverá ser capaz de viabilizar a execução de todos os procedimentos operacionais descritos neste anexo. As informações utilizadas na POC deverão, obrigatoriamente, ser de caráter fictício.

1.2. A Prova de Conceito deve ser iniciada em até 5 (cinco) dias úteis a partir da convocação pela CONTRATANTE, e ser finalizada em até 5 (cinco) dias úteis.

1.3. A Prova de Conceito poderá ser acompanhada por todos os interessados, independentemente de sua classificação, bastando para tanto o interessado comunicar formalmente o pregoeiro do interesse.

1.4. Os outros licitantes que tenham participado da etapa competitiva e demais interessados que desejem acompanhar a sessão, poderão indicar um representante para acompanhamento, devendo para tanto enviar para o e-mail da Comissão Permanente de Licitação (cdl@proderj.rj.gov.br) até as 16hs do último dia útil que antecede a sessão de teste. No e-

mail deverão constar: dados da empresa interessada (nome e contato), de seu representante (nome e contato) para o devido credenciamento.

1.5. Para a prova de conceito o licitante classificado em primeiro lugar, deverá apresentar a solução de forma presencial, preferencialmente virtualizado, em lugar definido pela CONTRATANTE. A solução deverá ser acessada remotamente no ambiente da licitante.

1.6. Se a solução apresentada não for aprovada, a proposta da empresa será eliminada, e se procederá à realização da convocação da empresa subsequente, nos mesmos moldes da anterior, observando a ordem de classificação estabelecida no final do processo competitivo, e assim sucessivamente, até a apuração de uma proposta que atenda às especificações.

1.7. O acesso ao ambiente utilizado para a Prova de Conceito deverá ser franqueado à técnicos do PRODERJ e mantido durante toda a fase de Prova de Conceito para que sejam efetuadas as confrontações técnicas necessárias. O acesso poderá ser revogado pela empresa ao término da Prova de Conceito, cabendo a ela a responsabilidade pela retirada.

1.8. A prova de conceito (POC) deve ser precedida em horário comercial, das 9h às 12h e das 14h às 18h.

1.9. Após a realização da Prova de Conceito, será emitido relatório resumido de análise, descrevendo as atividades realizadas e contendo a aprovação ou não da proposta.

1.10. A prova será realizada no ambiente do PRODERJ, a ser definido no ato da convocação em um dos endereços abaixo mencionados:

a) Data Center – Universidade do Estado do Rio de Janeiro (UERJ). End.: R. São Francisco Xavier 524, 2º andar, bloco “F”, Maracanã, Rio de Janeiro – RJ, CEP: 20550-013;

b) Data Center – Centro Integrado de Comando e Controle (CICC). End.: Rua Carmo Neto s/nº, Cidade Nova, Rio de Janeiro – RJ - CEP 20210-051; ou

c) Sede – Centro de Tecnologia da Informação e Comunicação do Governo do Estado do Rio de Janeiro (PRODERJ). End.: R. da Conceição 69, 24º e 25º andar, Centro, Rio de Janeiro – RJ CEP 20051-011.

Relação de Comprovação de Atendimento aos Requisitos

ITEM	REQUISITOS TÉCNICOS	ATENDE	
		SIM	NÃO
1	Funcionalidade de detecção (sensor de detecção) entregue em formato de appliance física.		
2	A plataforma permite a retenção de logs de eventos e fluxos de rede por um período de até 90 dias.		
3	Os sensores de detecção possuem capacidade de alta-disponibilidade em HA com funções de MASTER-SLAVE.		
4	A solução executa o correlacionamento dos eventos para detectar táticas, técnicas e procedimentos de ataques, identificados pela modelagem de ameaças desenvolvida pelo MITRE.		
5	A solução permite a integração com terceiros para resposta automatizada de ameaças através de conexão via API, WEB ou SSH.		
5	A solução possui capacidade autônoma ou componente dedicado para resposta automatizada na rede para execução de bloqueios de IP e/ou reset de sessão.		
7	A solução possui a capacidade de detecção de ataques desconhecidos sem a necessidade de criação manual de políticas avançadas para essas detecções, sendo uma função nativa.		
8	A solução possui modelos para apresentar fases da cadeia de ataque (attack kill-chain) e determinar em qual fase se encontram as ameaças detectadas.		
9	A solução apresenta painel central com centralização de todas as ameaças de todos os sensores existentes no ambiente além de correlação entre eles e com dados recebidos de diferentes fontes externas.		

10	A solução possui função de honeypot permitindo criar ambientes de “emboscada” emulados diretamente na solução, e registar tentativas de ataques a esses ambientes.		
11	A solução possui componente funcional de criação, execução e monitoramento de playbooks (fluxos de trabalho) para automações diversas, com capacidades de:		
12	Correlação de diversas fontes de dados e criação de condições;		
13	Enriquecimento de dados;		
14	Criação de filtros em logs;		
15	Os sensores de detecção possuem fontes de alimentação redundantes.		
16	A solução possui captura de pacote dos eventos detectados.		
17	A solução apresenta capacidade de sandbox para avaliação de artefactos em nuvem.		
18	A solução possui suporte ao protocolo Netflow e apresentação desses fluxos de rede detectados com detalhes desses fluxos.		
19	A solução permite pesquisa em logs por palavras-chave, termos e filtros baseados em SPL, Elastic ou similar.		
20	A solução faz uso do tráfego de rede através de espelhamento de tráfego (cópia/mirror) enviado ao sensor de deteção, sem a necessidade de instalação de componentes adicionais em máquinas ou servidores.		
REQUISITOS FUNCIONAIS			
21	A solução permite o uso de perfis de acesso com no mínimo:		
22	Alta administração (coordenadores, gestores);		
23	Equipe técnica (painel completo e detalhado);		
24	Auditores (auditor interno, auditores externos etc.).		
25	A solução possui visão agregada de eventos, com mínimo de:		
26	Agregação por eventos do mesmo endereço IP de atacante;		
27	Agregação por eventos que tiveram o mesmo endereço IP como vítima;		
28	Agregação por eventos com mesmo nome/tipo.		
29	A solução possui capacidade de geração de relatórios com informações de ameaças e informações de respostas aos incidentes.		
30	A solução possui painel central que receba logs encaminhados de diversas fontes com capacidade de reconhecimento desses logs e correlação avançada.		
31	A solução realizada reconhecimento e transformação dos logs (pharsing e normalização) de diversas fontes via syslog e com configuração via interface gráfica, sem necessidade de uso de linhas de comandos para configuração.		
32	A solução apresenta cenários pré-definidos ou customizados para casos especiais, como a criação de visualização especial para eventos de ransomware e mineração, mostrando cada etapa da cadeia destes ataques.		
33	As soluções contêm fonte de threat intelligence para apresentação de ameaças que ocorreram na web.		
34	A solução apresenta caminho inicial a ser tomado para resolução da ameaça encontrada.		
35	A solução deve aprender com o trafégo identificado e criar uma baseline que possibilite a identificação do padrão de conexão, além de alertar fugas de comportamento.		
36	A solução possui capacidade de detecção de ameaças/eventos baseado em comportamento.		
37	Todos os itens ofertados possuem integração nativa entre si e não necessitam e integração manual avançada ou customização.		

38	A solução suporta o tráfego de pacotes em Jumbo Frame.		

Rio de Janeiro, na data da assinatura eletrônica

Documento assinado eletronicamente por **Rodolfo Targino de Araujo**, **Assistente**, em 23/03/2026, às 14:14, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Luís Cláudio Marinho Coelho**, **Gerente**, em 23/03/2026, às 14:26, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor-Chefe**, em 23/03/2026, às 14:27, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Roberto Charles Vilas**, **Diretor**, em 23/03/2026, às 14:28, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 23/03/2026, às 14:33, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **128113468** e o código CRC **E52E1AF4**.

Governo do Estado do Rio de Janeiro
Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro
Vice Presidência de Tecnologia

ANEXO IV - PROVA DE CONCEITO II

1. INTRODUÇÃO

1.1. A prova de conceito consistirá na apresentação do funcionamento das Plataformas a serem contratadas, possuindo cunho de execução **facultativo**, sob a condição de avaliação somente quando exigido para a complementação do entendimento técnico acerca da oferta disponibilizada pelas licitantes.

1.1.1. O referido LICITANTE será convocado no prazo de até 10 (dez) dias úteis, a contar da aprovação da sua documentação de habilitação, para uma reunião preparatória (que poderá ocorrer em plataforma virtual), onde serão definidas as providências necessárias ao ambiente de teste da POC. Nessa reunião o LICITANTE deverá informar os requisitos necessários para a instalação do ambiente de teste a serem disponibilizados pelo PRODERJ conforme entendimento durante a reunião. Entende-se por "requisitos necessários":

a) Disponibilização de máquinas virtuais e/ou estações de trabalho, projetor e link de internet;

b) Criação de VLAN's e/ou disponibilização de endereços IP e entrada de DNS;

c) Criação de servidores de aplicação web;

d) Criação de usuários no AD e/ou modificações de regras de firewall, IPS, etc;

e) Caso seja aplicável, a disponibilização de periféricos, tais como: cabos, switches e outros componentes semelhantes não mencionados.

1.1.2. Nesta reunião preparatória, o LICITANTE deverá, sob pena de desclassificação, entregar os documentos da(s) solução(ões) que permitam comprovar o atendimento aos requisitos técnicos constantes do Anexo I deste documento, apresentando no mínimo:

a) ID do requisito;

b) Descrição do requisito;

c) Nome do produto ofertado (modelo, marca e fabricante);

d) Nome do documento de referência onde é possível verificar evidência do atendimento do requisito;

e) Página do documento referência onde é possível verificar evidência do atendimento do requisito;

f) Outras informações necessárias.

1.1.3. O LICITANTE será responsável por todos os custos inerentes à realização da prova de conceito, tais como despesas com viagens, estadas, equipe técnica, equipamentos, assim como, pela geração dos dados simulados que deverá ser capaz de viabilizar a execução de todos os procedimentos operacionais descritos neste anexo. As informações utilizadas na POC deverão, obrigatoriamente, ser de caráter fictício.

1.2. A Prova de Conceito deve ser iniciada em até 5 (cinco) dias úteis a partir da convocação pela CONTRATANTE, e ser finalizada em até 5 (cinco) dias úteis.

1.3. A Prova de Conceito poderá ser acompanhada por todos os interessados, independentemente de sua classificação, bastando para tanto o interessado comunicar formalmente o pregoeiro do interesse.

1.4. Os outros licitantes que tenham participado da etapa competitiva e demais interessados que desejem acompanhar a sessão, poderão indicar um representante para acompanhamento, devendo para tanto enviar para o e-mail da Comissão Permanente de Licitação (cdl@proderj.rj.gov.br) até as 16hs do último dia útil que antecede a sessão de teste. No e-mail deverão constar: dados da empresa interessada (nome e contato), de seu representante (nome e contato) para o devido credenciamento.

1.5. Para a prova de conceito o licitante classificado em primeiro lugar, deverá apresentar a solução de forma presencial, preferencialmente virtualizado, em lugar definido pela CONTRATANTE. A solução deverá ser acessada remotamente no ambiente da licitante.

1.6. Se a solução apresentada não for aprovada, a proposta da empresa será eliminada, e se procederá à realização da convocação da empresa subsequente, nos mesmos moldes da anterior, observando a ordem de classificação estabelecida no final do processo competitivo, e assim sucessivamente, até a apuração de uma proposta que atenda às especificações.

1.7. O acesso ao ambiente utilizado para a Prova de Conceito deverá ser franqueado à técnicos do PRODERJ e mantido durante toda a fase de Prova de Conceito para que sejam efetuadas as confrontações técnicas necessárias. O acesso poderá ser revogado pela empresa ao término da Prova de Conceito, cabendo a ela a responsabilidade pela retirada.

1.8. A prova de conceito (POC) deve ser precedida em horário comercial, das 9h às 12h e das 14h às 18h.

1.9. Após a realização da Prova de Conceito, será emitido relatório resumido de análise, descrevendo as atividades realizadas e contendo a aprovação ou não da proposta.

1.10. A prova será realizada no ambiente do PRODERJ, a ser definido no ato da convocação em um dos endereços abaixo mencionados:

a) Data Center – Universidade do Estado do Rio de Janeiro (UERJ). End.: R. São Francisco Xavier 524, 2º andar, bloco “F”, Maracanã, Rio de Janeiro – RJ, CEP: 20550-013;

b) Data Center – Centro Integrado de Comando e Controle (CICC). End.: Rua Carmo Neto s/nº, Cidade Nova, Rio de Janeiro – RJ - CEP 20210-051; ou

c) Sede – Centro de Tecnologia da Informação e Comunicação do Governo do Estado do Rio de Janeiro (PRODERJ). End.: R. da Conceição 69, 24º e 25º andar, Centro, Rio de Janeiro – RJ CEP 20051-011.

1.11. Será necessária a realização de prova de conceito (POC) para os itens:

1.11.1. Do Lote 02: Item 12 - Interceptador do tráfego virtualizado avançado.

1.12. Ademais, exibimos o rol de itens que deverão ser comprovados durante a prova de conceito. Caso a licitante requisite a inserção de itens complementares ao entendimento da solução, a solicitação por adição de novos itens deverá ocorrer em fase prévia a disponibilização da solução no ambiente do PRODERJ.

1.13. Foram removidos do escopo de testes requisitos que possam gerar custos adicionais para a operacionalização da solução, por parte das licitantes.

1.14. Foram removidos do escopo de testes, quaisquer requisitos que possam gerar impactos na rede do PRODERJ.

1.15. Caso seja necessário empregar qualquer software ou plataforma complementar para o entendimento correto de uma funcionalidade, será admitido o seu fornecimento em versão “trial”, “freeware” ou qualquer outro modelo que não gere custos adicionais.

1.16. O espectro de requisitos expostos a seguir já fora pré-selecionado quanto aos itens que requisitam uma real apuração de funcionamento em tempos de execução. Os requisitos não determinados serão apurados através de documentação técnica e oficial da fabricante da solução ofertada durante a fase de habilitação.

1.17. Para testes baseados em plataforma de virtualização, o PRODERJ disponibilizará até 6 (seis) máquinas virtuais baseadas em ambiente VMware, por Lote a ser testado.

1.18. Para a demonstração da capacidade da solução, não será exigida a geração de tráfego o qual deverá fluir pelos componentes. A demonstração da habilidade de dispor configurações técnicas em conformidade com as especificações requisitadas será suficiente para atestar a capacidade técncio operacional da oferta.

1.19. Todas as atividades executadas deverão ser registradas e entregues a equipe técnica do órgão para análise posterior, em formato de relatório, visando a melhor conclusão do teste de homologação.

1.20. Por registro, entende-se como a gravação dos testes executados (captura das telas de gerência), ou a gravação do ambiente de testes (transmissão síncrona e gravada por ferramenta de colaboração), para comprovar a participação da equipe técnica do órgão e da licitante ofertante do menor preço durante a execução dos testes.

1.21. Para a execução dos testes, serão aceitos casos de uso que fornecem o mesmo resultado esperado, mesmo que não explicitamente idênticos ao requisito solicitado.

RELAÇÃO DE COMPROVAÇÃO DE ATENDIMENTO AOS REQUISITOS

LOTE 02 - ITEM 12 – INTERCEPTADOR DO TRÁFEGO VIRTUALIZADO AVANÇADO		ATENDE?	
ITEM	**FUNCIONALIDADE / CARACTERÍSTICA**	**SIM**	**NÃO**
1	Deverá ser fornecido no formato de appliance virtual, com seu licenciamento na modalidade de subscrição.		
2	Deverá ser do mesmo fabricante ofertado para o Equipamento para a Interceptação do Tráfego.		
3	A solução entregue deverá estar licenciada para processar, no mínimo, 50 TB (cinquenta terabytes) de dados por dia.		
4	Deverá implementar a coleta de tráfego dentro do mundo virtual (tráfego entre VMs) através de Interceptadores Virtualizados ou Virtual TAPs.		
5	Deverá suportar o monitoramento de múltiplos switches virtuais distribuídos simultaneamente.		
6	Deverá suportar a identificação automática das VMs que devem ser monitoradas através das definições de regras de seleção do tráfego que deve ser monitorado.		
7	Deverá implementar a mobilidade das máquinas virtuais, de forma que quando ocorrer uma migração de uma VM para outro host, todas as políticas relacionadas a esta VM continuem sendo aplicadas sem a necessidade de reconfiguração manual.		
8	Deverá permitir a visualização e monitoramento, através de um gerencia centralizada, de todos os appliances virtuais componentes da solução.		
9	Deverá permitir a pré-filtragem do tráfego nos TAPs virtuais antes de enviá-lo para as ferramentas de segurança.		
10	Deverá permitir a visualização e monitoramento da taxa de tráfego e o resumo do volume de tráfego agregado.		
11	Deve implementar a funcionalidade de desencapsulamento de cabeçalhos L2GRE, VXLAN, ERSPAN e GENEVE dos pacotes de rede.		
12	Deve implementar a funcionalidade de encapsulamento dos pacotes de rede com o protocolo L2GRE ou VXLAN.		
13	Deve implementar a funcionalidade de mascaramento de dados nos pacotes para garantir a privacidade de dados.		
14	Deve implementar a funcionalidade de slicing (corte) dos pacotes, reduzindo o volume de tráfego com payloads irrelevantes.		
15	Deve implementar o balanceamento de carga do tráfego para dois túneis L2GRE ou VXLAN diferentes.		
16	Deve implementar a filtragem do tráfego de rede baseado em aplicações (camada 7).		
17	A funcionalidade de filtragem por aplicação deve ser capaz de reconhecer a aplicação independentemente da porta TCP ou UDP.		
18	Deve enriquecer as informações de NetFlow com dados contextuais da camada de aplicação.		
19	Deve permitir o envio de metadados dados para até quatro coletores diferentes.		
20	Deve implementar o envio de dados em diferentes formatos, tais como IPFIX, CEF e JSON sobre HTTPS.		
21	A funcionalidade Packet De-Duplication deve permitir habilitar ou desabilitar a inspeção de, no mínimo, os seguintes campos para avaliar se é um pacote duplicado ou não:		

21.1	Número da Sequência TCP;		
21.2	VLAN ID.		
22	A funcionalidade Masking deverá ser capaz de trocar uma determinada informação como o CPF do usuário por outros caracteres (XXX.XXX.XXX-XX, por exemplo), de modo que essa informação específica seja protegida antes de ser enviada para as soluções.		

1.22. A equipe técnica elaborará relatório com o resultado da prova de conceito, informando se a solução apresentada pelo licitante provisoriamente classificado em primeiro lugar está ou não de acordo com os requisitos e funcionalidades estabelecidas.

1.23. Caso o relatório indique que a solução tecnológica está em conformidade com as especificações exigidas, o licitante será declarado vencedor do processo licitatório e, caso indique a não conformidade, o licitante será desclassificado do processo licitatório.

1.24. Caso o relatório indique que a solução foi aprovada com ressalvas, as não conformidades serão listadas e o licitante terá prazo de 3 (três) dias úteis, não prorrogáveis, a contar da data de ciência do respectivo relatório, para proceder aos ajustes necessários na solução e disponibilizá-la, para a realização de testes complementares, para aferição da correção ou não das inconformidades indicada.

1.25. Caso a licitante opte em não reexecutar as ressalvas, ela será desclassificada imediatamente. No caso, a próxima licitante será convocada.

1.26. Poderá ser considerada aprovada com ressalva a solução que, embora possua todas as funcionalidades previstas na Prova de Conceito, venha a apresentar falha durante o teste.

1.27. Caso o novo relatório indique a não conformidade da solução ajustada às especificações técnicas exigidas, a licitante será desclassificada do processo licitatório.

1.28. Não será aceita a proposta da licitante que tiver a Prova de Conceito rejeitada, que não a realizar ou que não a realizar nas condições estabelecidas no Termo de Referência.

1.29. No caso de desclassificação do licitante, o pregoeiro convocará o próximo licitante, obedecida a ordem de classificação, sucessivamente, até que um licitante cumpra os requisitos e funcionalidades previstas na Prova de Conceito.

1.30. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

1.31. Para acompanhamento será permitida a participação de até 2 (dois) representantes de cada empresa, devidamente cadastradas e participantes da licitação, e somente sob a condição de observador.

1.32. Será permitida a presença de até 2 (dois) representantes do fabricante para apoiar na execução dos testes.

1.33. Durante o período de testes, os participantes não poderão efetuar qualquer tipo de comunicação com os executores e nem com a equipe de TI do órgão gerenciador. Todavia, poderá ser utilizado material para a tomada de anotações dos eventos ocorridos durante os testes.

1.34. Fica vedada a realização de perguntas ou comentários durante a execução dos testes por parte dos demais licitantes.

1.35. Não será permitida, no momento de da prova de conceito, a interação entre os ouvintes com quaisquer participantes. Questões sobre o processo deverão seguir os trâmites de contato via responsável e em momento oportuno.

1.36. É vedado aos participantes ouvintes da da prova de conceito gravar a transmissão com pena de violação legal de propriedade intelectual.

Rio de Janeiro, na data da assinatura eletrônica

Documento assinado eletronicamente por **Rodolfo Targino de Araujo**, **Assistente**, em 23/03/2026, às 14:14, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Luís Cláudio Marinho Coelho**, **Gerente**, em 23/03/2026, às 14:26, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor-Chefe**, em 23/03/2026, às 14:27, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Roberto Charles Vilas**, **Diretor**, em 23/03/2026, às 14:28, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 23/03/2026, às 14:33, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **128113223** e o código CRC **7F8626F8**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro
Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro
Vice Presidência de Tecnologia

MAPA DE RISCOS

OBJETO

Solução de interceptação de tráfego, monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, com Instalação da Solução, incluindo hardware, software e demais componentes, bem como serviços de treinamento e garantia com manutenção do fabricante por 36 (trinta e seis) meses.

IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

No escopo da presente contratação, foram identificados os riscos inerentes ao negócio, os passíveis de comprometer o êxito do processo de contratação e os referentes à gestão contratual.

Cada risco identificado foi enquadrado conforme seu tipo (infraestrutura, segurança ou organizacional), considerando-se a probabilidade de ocorrência dos eventos, os possíveis danos potenciais em caso de acontecimentos, as possíveis ações preventivas e de contingências, bem como a identificação de responsáveis por ação. Para tanto, tais riscos foram classificados a partir da atribuição de valores aos níveis de probabilidade (P) e impacto (I), conforme tabela abaixo:

Escala Qualitativa de Classificação	
Classificação	**Valor**
Baixo	5
Médio	10
Alto	15

Em seguida, o produto obtido da relação entre a probabilidade e o impacto resultou na elaboração da Matriz Probabilidade x Impacto, instrumento responsável pela definição dos critérios quantitativos de classificação do nível de risco, a fim de direcionar as ações relacionadas aos riscos durante a fase de planejamento e gestão do contrato.

Probabilidade (P)	15	**75**	**150**	**225**
	10	**50**	**100**	**150**
	5	**25**	**50**	**75**

	5	10	15

Impacto (I)

Caso o risco se enquadre na região verde, seu nível de risco é entendido como baixo, logo, admite-se sua aceitação ou adoção das medidas preventivas, por meio do uso de controles de segurança. Se estiver na região amarela, entende-se como médio; e se estiver na região vermelha, entende-se como nível de risco alto. Nos casos de riscos classificados como médio e alto, deve-se adotar obrigatoriamente os controles de segurança previstos.

Uma vez definidos os riscos e seus níveis, indicou-se a resposta de ação correspondente a cada um deles, de acordo com o quadro abaixo:

Respostas aos riscos	
Evitar	Eliminar o risco, evitando-o totalmente.
Mitigar	Reduzir a probabilidade e/ou o impacto do risco, ação realizada independente do risco ocorrer ou não.
Transferir	Passar o custo da consequência para um terceiro.
Aceitação Ativa	Criar um plano de contingência para ser acionado, caso o risco ocorra.
Aceitação Passiva	Não tomar nenhuma ação preventiva, lidando com o problema apenas caso o risco ocorra.

A partir do percurso metodológico descrito, foram identificados os seguintes riscos:

Tabela de relação de riscos identificados						
Id	**Risco**	**Tipo de Risco**	**Probabilidade**	**Impacto**	**Nível de Risco (P X I)**	**Respostas aos Riscos**
R1	Dependência tecnológica a ser estabelecida entre a contratante e contratada	Risco de Infraestrutura	10	10	100	Mitigar/ Aceitação Ativa
R2	Especificação incorreta ou incompleta da solução desejada	Risco de Infraestrutura	5	15	75	Mitigar/ Aceitação Ativa
R3	Interrupção do serviço	Risco de Infraestrutura	5	15	75	Mitigar/ Aceitação Ativa

R4	Atraso ou suspensão no processo licitatório em face de impugnações	Risco organizacional	5	15	75	Evitar/ Aceitação Ativa
R5	Ausência de recursos orçamentários ou financeiros	Risco organizacional	5	15	75	Mitigar/ Aceitação Ativa
R6	Descumprimento das cláusulas contratuais pela contratada	Risco organizacional	5	15	75	Mitigar/ Aceitação Ativa
R7	Descumprimento dos níveis de serviço estabelecidos	Risco organizacional	5	15	75	Mitigar/ Aceitação Ativa
R8	**A empresa contratada não ter capacidade de entregar o objeto**	Risco organizacional	5	15	75	Mitigar/ Aceitação Ativa
R9	**Dificuldade na fiscalização do contrato**	Risco organizacional	10	15	150	Mitigar/ Aceitação Ativa

3. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

3.1. Riscos de Infraestrutura

Risco 1	**Risco:**		Dependência tecnológica a ser estabelecida entre a Contratante e a Contratada
	Probabilidade:		Média
	Impacto:		Médio
	Dano 1:		Dependência excessiva da solução.
	Dano 2:		Desuso da solução após término de contrato.
	Id	**Ação Preventiva**	**Responsável**

	1	Buscar e manter conhecimento sobre solução simular aos produtos contratados	Área Técnica
	2	Manter o conhecimento do serviço e dos processos de execução sob controle da Contratante, de modo a reduzir o risco de dependência em relação ao fornecedor.	Equipe de Fiscalização do Contrato
	3	Promover o monitoramento contínuo da execução contratual, por meio de registro histórico, com o objetivo de garantir a continuidade dos serviços e evitar sua interrupção de forma não programada.	Equipe de Fiscalização do Contrato
	Id	**Ação de Contingência**	**Responsável**
	1	Realização de novo procedimento licitatório com antecedência ante a impossibilidade de prorrogação do contrato atual.	Equipe de Licitação

Risco 2	**Risco:**	Especificação incorreta ou incompleta da solução desejada	
	Probabilidade:	Baixo	
	Impacto:	Alto	
	Dano 1:	Deficiência na execução dos serviços.	
	Dano 2:	Não atingimento completo dos resultados elencados nos artefatos de planejamento da contratação.	
	Id	**Ação Preventiva**	**Responsável**
	1	Garantir que o Estudo Técnico Preliminar seja elaborado de forma adequada, englobando todo o escopo necessário ao atingimento dos resultados esperados.	Equipe de Planejamento da Contratação
	2	Revisar cuidadosamente o Termo de Referência quando o objeto possuir especificações técnicas ou condições de fornecimento específicos.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Retornar à análise de viabilidade da contratação e verificar a solução que melhor atenda às necessidades de negócio.	Área Técnica e Área de Negócio

Risco 3	**Risco:**	Interrupção do serviço

	Probabilidade:	Baixa	
	Impacto:	Alto	
	Dano 1:	Interrupção da prestação dos serviços de atualização e da garantia , podendo gerar falhas de segurança e impossibilidade de atualização das versões.	
	Id	**Ação Preventiva**	**Responsável**
	1	Garantir que o Termo de Referência defina a aplicação de penalidades proporcionais em caso de interrupção abrupta dos serviços.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar as sanções administrativas previstas no Contrato.	Comissão de Fiscalização do Contrato
	2	Verificar junto à empresa as condições para o reestabelecimento da prestação do serviço.	Comissão de Fiscalização do Contrato
	3	Iniciar elaboração de novo procedimento licitatório, caso haja rescisão contratual.	Equipe de Licitação

3.2. Riscos Organizacionais

Risco 4	**Risco:**	Atraso ou suspensão no processo licitatório em face de impugnações e recursos	
	Probabilidade:	Alta	
	Impacto:	Alto	
	Dano 1:	Demora ou impedimento da contratação.	
	Id	**Ação Preventiva**	**Responsável**
	1	Verificar e avaliar os pontos que levam à licitação deserta/frustrada, bem como impugnações e recursos em contratações similares, para evitar que estas causas sejam reproduzidas no procedimento licitatório.	Equipe de Planejamento da Contratação
	2	Dar celeridade ao processo licitatório, dentro das condições impostas no edital.	Equipe de Licitação
	3	Estabelecer condições técnico-administrativas no Termo de Referência que não restrinjam a competitividade do certame.	Área Técnica

	4	Revisar os artefatos de planejamento da contratação.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	2	Alteração de condições técnico-administrativas do Termo de Referência, a fim de que possam permitir o andamento do processo licitatório, desde que não desnaturem o objeto.	Equipe de Planejamento da Contratação

Risco 5	**Risco:**	Ausência de recursos orçamentários ou financeiros	
	Probabilidade:	Baixa	
	Impacto:	Alto	
	Dano 1:	Atraso e/ou interrupção do processo de contratação.	
	Dano 2:	Perda do acesso das subscrições.	
	Dano 3:	Perda da possibilidade de atualizar as licenças perpétuas pela não realização de pagamento em prazo superior a 90 (noventa) dias.	
	Id	**Ação Preventiva**	**Responsável**
	1	Verificar o alinhamento estratégico da contratação ao PEDTIC e aos documentos de planejamento do órgão (PAC).	Equipe de Planejamento da Contratação
	2	Reservar os recursos orçamentários.	Ordenador de Despesas
	3	Expor à Alta Administração, bem como ao Ordenador de Despesa, a importância e relevância da contratação.	Área de Negócio
	Id	**Ação de Contingência**	**Responsável**
	1	Verificar possibilidade de operação de crédito para execução da despesa.	Ordenador de Despesas
	2	Realizar novo procedimento licitatório para contratação do Objeto	Equipe de Licitação

Risco 6	**Risco:**	Descumprimento das cláusulas contratuais pela Contratada
	Probabilidade:	Baixa
	Impacto:	Alto

	Dano 1:	Não entrega dos serviços contratados.
	Dano 2:	Atraso no início da execução dos serviços.
	Dano 3:	Qualidade insatisfatória dos serviços prestados.
	Dano 4:	Descontinuidade dos serviços.
	Dano 5:	Falta de efetividade da contratação.

Id	**Ação Preventiva**	**Responsável**
1	Acompanhar a execução dos serviços, aferindo se os requisitos previstos pelo instrumento contratual e pelo Termo de Referência estão sendo cumpridos de acordo com os níveis de qualidade estabelecidos.	Comissão de Acompanhamento e Fiscalização do Contrato
2	Designar Comissão de Acompanhamento e Fiscalização do Contrato composta por servidores capazes de fiscalizar efetivamente o contrato.	Alta Gestão

Id	**Ação de Contingência**	**Responsável**
1	Notificar formalmente a Contratada quando cláusulas do contrato forem descumpridas.	Comissão de Acompanhamento e Fiscalização do contrato
2	Aplicar de multa moratória e as penalidades previstas no contrato, de forma a coibir a reincidência de descumprimentos contratuais.	Comissão de Acompanhamento e Fiscalização do contrato
3	Rescindir o contrato unilateralmente e iniciar novo processo de contratação, utilizando os artefatos de planejamento produzidos, com as atualizações baseadas na experiência adquirida no processo de gestão e fiscalização.	Comissão de Acompanhamento e Fiscalização do contrato / Alta Gestão / Equipe de Planejamento da Contratação

Risco 7	**Risco:**	Descumprimento dos níveis de serviço estabelecidos
	Probabilidade:	Baixa
	Impacto:	Alto
	Dano 1:	Impacto negativo sobre a qualidade dos serviços prestados, não atendendo aos requisitos estabelecidos no Termo de Referência.

Id	**Ação Preventiva**	**Responsável**

	1	Atribuir multa moratória e sanções razoáveis no Termo de Referência que disciplinem a continuidade dos serviços de forma satisfatória.	Comissão de Acompanhamento e Fiscalização do contrato
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar as sanções administrativas, conforme previstas no Termo de Referência e no Contrato.	Comissão de Acompanhamento e Fiscalização do contrato

Risco 8	**Risco:**	**A empresa contratada não ter capacidade de entregar o objeto.**	
	Probabilidade:	Baixa	
	Impacto:	Alto	
	Dano 1:	Fracasso do processo licitatório Não alcançar os objetivos propostos Perdas financeiras causadas pela utilização de tecnologias mais caras durante um período mais prologando	
	Id	**Ação Preventiva**	**Responsável**
	1	O termo de referência deverá solicitar atestado de capacidade técnica capaz de determinar se a empresa vencedora do certame realmente está capacitada a fornecer o objeto contratado.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar punições cabíveis a CONTRATADA que não cumprir os termos estabelecidos no termo de referência e no contrato. Tomar ações jurídicas cabíveis caso a empresa não comprove que os atestados entregues são verdadeiros.	Área técnica e jurídica.

Risco 9	**Risco:**	**Dificuldade na fiscalização do contrato**
	Probabilidade:	Médio
	Impacto:	Alto
	Dano 1:	Não alcançar os objetivos da contratação

	Realizar pagamentos não condizentes com os serviços prestados.	
Id	**Ação Preventiva**	**Responsável**
1	O termo de referência deverá estabelecer um instrumento de medição de resultados eficiente, capaz de estabelecer critérios objetivos na medição e avaliação dos serviços prestados.	Equipe de Planejamento da Contratação
Id	**Ação de Contingência**	**Responsável**
1	Aplicar glosas e sanções previstas no IMR (Instrumento de medição de resultados)	Comissão de Acompanhamento e Fiscalização do contrato

Rio de Janeiro, na data da assinatura eletrônica.

Documento assinado eletronicamente por **Rodolfo Targino de Araujo**, **Assistente**, em 23/03/2026, às 14:15, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Luís Cláudio Marinho Coelho**, **Gerente**, em 23/03/2026, às 14:26, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor-Chefe**, em 23/03/2026, às 14:27, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Roberto Charles Vilas**, **Diretor**, em 23/03/2026, às 14:28, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 23/03/2026, às 14:33, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **128113966** e o código CRC **C374D660**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone: