



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

TERMO DE REFERÊNCIA

JUSTIFICATIVA DA NECESSIDADE E DO TIPO DE SOLUÇÃO ESCOLHIDA

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.

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.

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.

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.

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.

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.

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.

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.

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).

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.

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.

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.

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

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.
- **Deteção 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.

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.”

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.

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.

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.

DEFINIÇÃO DO OBJETO

Registro de Preços para a contratação de empresa especializada na aquisição de 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, e serviços de implantação, treinamento, incluindo serviços de garantia, conforme especificações e quantidades estabelecidas neste Termo de Referência e nos requisitos da contratação descritos no Estudo Técnico Preliminar, conforme condições definidas no ANEXO I, deste documento.

O Prazo de garantia do fornecedor será de 36 (trinta e seis) meses.

INSTRUMENTOS DE PLANEJAMENTO

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

ID PCA no PNCP: [442498600000171-0-000030/2026](#);

Data de publicação no PNCP: 01/08/2025;

ID dos itens no PCA: Vide Tabela do Item 4



Alinhamento Estratégico

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, suprimindo 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).

  Portal Nacional de Contratações Públicas

Buscar no PNCP



 Entrar

15918

7035 - ACESSORIOS PARA PROCESSAMENTO DE DADOS


R\$ 8.540.566,48

01/02/2026

  Portal Nacional de Contratações Públicas

Buscar no PNCP




 Entrar

15932

0349 - SERVICOS. ADMINISTRACAO. DESENVOLVIMENTO DE APLICACOES

R\$ 2.591.174,40

01/02/2026

  Portal Nacional de Contratações Públicas

Buscar no PNCP





 Entrar

15931

0335 - SERVICOS DE TREINAMENTO

R\$ 20.778,74

01/02/2026

  Portal Nacional de Contratações Públicas

Buscar no PNCP



 Entrar

15936

7011 - COMPONENTES DE REDE

R\$ 553.301,32

01/02/2026

  Portal Nacional de Contratações Públicas

Buscar no PNCP



 Entrar

15921

0193 - SERVICOS DE LOCACAO DE SOFTWARE


R\$ 238.043,16

01/02/2026

  Portal Nacional de Contratações Públicas

Buscar no PNCP



 Entrar

15923

0193 - SERVICOS DE LOCACAO DE SOFTWARE

R\$ 8.321.480,60

01/02/2026

  Portal Nacional de Contratações Públicas

Buscar no PNCP



 Entrar

15927

0193 - SERVICOS DE LOCACAO DE SOFTWARE


R\$ 141.369,28

01/02/2026

  Portal Nacional de Contratações Públicas

Buscar no PNCP



 Entrar

15935

0193 - SERVICOS DE LOCACAO DE SOFTWARE

R\$ 659.393,28

01/02/2026



15937

7011 - COMPONENTES DE REDE

R\$ 1.021.460,00

01/02/2026



15933

7011 - COMPONENTES DE REDE

R\$ 554.787,52

01/02/2026



15924

0193 - SERVICOS DE LOCACAO DE SOFTWARE

R\$ 383.652,46

01/02/2026



15938

0193 - SERVICOS DE LOCACAO DE SOFTWARE

R\$ 882.161,28

01/02/2026



15919

7010 - EQUIPAMENTOS DE PROCESSAMENTO DE DADOS

R\$ 15.333,00

01/02/2026



15928

7011 - COMPONENTES DE REDE

R\$ 40.506,24

01/02/2026



15925

7011 - COMPONENTES DE REDE

R\$ 166.279,04

01/02/2026



15916

7011 - COMPONENTES DE REDE

R\$ 55.303,04

01/02/2026



15922

7011 - COMPONENTES DE REDE

R\$ 323.633,76

01/02/2026

15915

6099 - ACESSORIOS E ARTIGOS DE FIBRA OPTICA

R\$ 26.301,28

01/02/2026

15934

6099 - ACESSORIOS E ARTIGOS DE FIBRA OPTICA

R\$ 92.590,56

01/02/2026

15926

6099 - ACESSORIOS E ARTIGOS DE FIBRA OPTICA

R\$ 40.848,32

01/02/2026

15930

6099 - ACESSORIOS E ARTIGOS DE FIBRA OPTICA

R\$ 155.535,04

01/02/2026

15929

0349 - SERVICOS, ADMINISTRACAO, DESENVOLVIMENTO DE APLICACOES

R\$ 1.379.970,84

01/02/2026

15917

0193 - SERVICOS DE LOCACAO DE SOFTWARE

R\$ 9.043.158,48

01/02/2026

15920

0349 - SERVICOS, ADMINISTRACAO, DESENVOLVIMENTO DE APLICACOES

R\$ 2.165.846,76

01/02/2026

ESPECIFICAÇÃO DO BEM E DO SERVIÇO CONFORME CATÁLOGO ELETRÔNICO DE PADRONIZAÇÃO DE COMPRA

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
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

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
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
LOTE II					
4	196478	15936	Equipamento para a interceptação do tráfego	Unidade	Aquisição de Equipamento
5	195071	15921	Licenciamento de desduplicação do tráfego.	Unidade	Subscrição de Licença por 36 meses
6	195072	15923	Licenciamento avançado de descrição do tráfego.	Unidade	Subscrição de Licença por 36 meses
7	195073	15927	Licenciamento avançado de análise de aplicações.	Unidade	Subscrição de Licença por 36 meses
8	195074	15935	Licenciamento avançado de análise de metadados.	Unidade	Subscrição de Licença por 36 meses
9	193207	15937	Módulo de expansão do processamento.	Unidade	Aquisição de Equipamento
10	123672	15933	Módulo de expansão para a captura do tráfego “inline”.	Unidade	Aquisição de Equipamento
11	195075	15924	Licenciamento para o gerenciamento centralizado da solução.	Unidade	Subscrição de Licença por 36 meses
12	195076	15938	Interceptor do tráfego virtualizado avançado.	Unidade	Subscrição de Licença por 36 meses
13	196651	15919	Chassi para interconector passivo de interceptação do tráfego - interfaces ópticas	Unidade	Aquisição de Equipamento
14	196668	15928	Interconector passivo de interceptação do tráfego – interfaces SFP	Unidade	Aquisição de Equipamento
15	196641	15925	Interconector passivo de interceptação do tráfego – interfaces QSFP	Unidade	Aquisição de Equipamento
16	196667	15916	Interconector passivo de interceptação do tráfego – interfaces RJ-45	Unidade	Aquisição de Equipamento
17	196499	15922	Concentrador de Tráfego de Segurança.	Unidade	Aquisição de Equipamento
18	195083	15915	Transceiver tipo 1 – 1 Gbps ethernet	Unidade	Aquisição de Equipamento
19	195084	15934	Transceiver tipo 2 – 10 Gbps ethernet	Unidade	Aquisição de Equipamento
20	195085	15926	Transceiver tipo 3 – 25 Gbps ethernet	Unidade	Aquisição de Equipamento
21	195086	15930	Transceiver tipo 4 – 100 Gbps ethernet	Unidade	Aquisição de Equipamento
22	196666	15929	Serviço técnico especializado para a solução de interceptação de tráfego.	UST	Sob Demanda
LOTE III					
23	195077	15917	Licenciamento Elastic Enterprise On-Premises.	Unidade	Subscrição de Licença por 36 meses
24	195080	15920	Serviço técnico especializado para o Licenciamento Elastic Enterprise On-Premises.	UST	Sob Demanda

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, com Instalação da Solução."), mas também todos os componentes físicos, lógicos e de serviço necessários para a sua implementação e operação eficaz.

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, controladores 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, descritografia, 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.

O item 11 do Estudo Técnico Preliminar traz informações complementares dos itens que compõem o objeto.

DESCRIÇÃO PORMENORIZADA CONSIDERANDO TODO O CICLO DE VIDA DO OBJETO A SER CONTRATADO

Trata-se de objeto que abrange bens e serviços de natureza comum, conforme o parágrafo único do art. 6º, XIII, da Lei nº 14.133/2021, tendo em vista que seus padrões de desempenho e qualidade estão objetivamente definidos no edital, com base em especificações técnicas amplamente utilizadas no mercado.

O ciclo de vida de um ativo de TIC, exigirá várias formas de serviço para permanecer funcionando de maneira ideal. Isso pode incluir manutenção contínua, atualizações ocasionais ou até mesmo reparos de emergência. Os membros da equipe precisam ter um tempo programado dedicado regularmente para garantir que essas medidas sejam tomadas para cada ativo individualmente, a fim de assegurar que funcione da forma mais eficiente possível.

A vida útil de um servidor é, em média, 3 anos. Quando o fabricante do servidor continua a produzir componentes, estendendo sua garantia, é possível que um servidor dure 5 anos. A completude das especificações técnicas estão descritas no Anexo I - Especificações Técnicas do Objeto.

DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

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.

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.

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.

Características Gerais

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.

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

MODELO DE EXECUÇÃO DO OBJETO

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.

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.

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.

Regime de execução:

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);

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);

JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

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.

Apresentamos a justificativa para essa divisão:

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

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.

Agrupamento de Componentes de Infraestrutura e Licenciamentos Necessários (Lote II)

Lote II agrupa todos os itens para o monitoramento. Inclui itens como equipamentos de interceptação de tráfego, diversos tipos de licenciamentos avançados (desduplicação, descritografia, 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.

Aquisição de Plataforma de Dados e Serviço Associado (Lote III)

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.

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, conseqüentemente, 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.

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.

PRAZOS DE INÍCIO E TÉRMINO DA PRESTAÇÃO DO SERVIÇO OU DE EXECUÇÃO DO OBJETO CONTRATUAL

Prazo do contrato e possibilidade de prorrogação

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.

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 nº 14.133/2021

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.

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 do 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.

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 do 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 nº 14.133/2021, desde que observadas as condições previstas no Contrato, e mediante a celebração de termo aditivo.

Prazos e condições de entrega dos bens e serviços

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).

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).

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.

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 serviço, que poderão ser emitidas após a divulgação do contrato no Portal Nacional de Compras Públicas (PNCP).

INDICAÇÃO DOS LOCAIS DE ENTREGA DOS PRODUTOS OU DA EXECUÇÃO DOS SERVIÇOS

O endereço de entrega dos bens do item 1 do Lote I, item 4, 9 e 10 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.

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;

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.

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.

REGRAS PARA O RECEBIMENTO PROVISÓRIO E DEFINITIVO

O objeto do contrato será recebido, na seguinte forma:

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):

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;

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;

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):

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;

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;

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

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;

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.

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):

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;

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.

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.

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.

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.

DEFINIÇÃO DAS CONDIÇÕES DOS SERVIÇOS DE CAPACITAÇÃO, MANUTENÇÃO, ASSISTÊNCIA TÉCNICA, SUPORTE E GARANTIA DOS BENS E SERVIÇOS

Requisitos de Capacitação

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.

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

A CONTRATADA deverá fornecer apostilas e vídeoaula contendo o material necessário a capacitação ofertada;

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.

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

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

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;

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

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

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

Os profissionais responsáveis por ministrar a capacitação deverão conhecer todos os aspectos técnicos e funcionais da solução aqui especificada, com experiência comprovada em capacitações no uso da solução.

A CONTRATADA será responsável pelas despesas relativas à participação de seus instrutores, tais como hospedagem, transporte, diárias, etc.

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.

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

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

Requisitos de Manutenção

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 suporte, atualização, e suporte técnico, por 36 (trinta e seis) meses.

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.

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).

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.

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).

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.

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.

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

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.

Requisitos de Garantia/ Suporte Técnico

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.

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;

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

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;

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;

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:

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

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;

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;

Vulnerabilidades (SQL Injection, etc);

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

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

O suporte técnico deverá:

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;

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

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

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

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

Anormalidade observada;

Nome do responsável pela solicitação do chamado técnico;

Sistema/versão/módulo/item;

Natureza do problema;

Descrição da natureza enfrentada.

O atendimento técnico deverá atender os seguintes requisitos técnicos:

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

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;

O atendimento de Suporte 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.

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

Identificação do chamado;

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

Identificação do defeito;

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

Atualizações de software/versões realizadas;

Acionamentos feitos à equipe da CONTRATADA;

Relatórios Extraordinários.

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.

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

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

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

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

Prestar assessoria para adequação do sistema à legislação vigente.

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.

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.

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

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.

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.

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

METODOLOGIA DE AVALIAÇÃO DA QUALIDADE E ACEITE DO OBJETO EXECUTADO, E, QUANDO SE TRATAR DE SERVIÇOS E FOR APLICÁVEL, O ACORDO DE NÍVEL DE SERVIÇO – ANS

Para os itens 1 do Lote I e 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.

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, e" do subtópico 13.19 deste documento, verificados durante o período.

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%

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.

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.

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

O descumprimento deste acordo de nível de serviço, notadamente quanto ao cumprimento dos prazos, ensejará as sanções previstas no subtópico 13.19 deste documento.

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;

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

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.

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).

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

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.

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.

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

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

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

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

Sanções

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

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.

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.

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.

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.

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;

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

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

CRITÉRIOS DE MEDIÇÃO, DE PAGAMENTO, CONDIÇÕES DE AQUISIÇÃO E REAJUSTAMENTO DO CONTRATO

Do Pagamento:

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:

Em 1 (uma) parcela, 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).

Parcelado, sob demanda, de acordo com cada 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).

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 recusa 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**.

14.2.3. 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, bem ainda no art. 140, II, alínea b, da Lei nº 14.133/2021 e nos arts. 20 e 22, XXIII do Decreto estadual nº 48.817/2023.

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

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

14.2.5. Recebida a Nota Fiscal ou Fatura, 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 o poder público, observadas as abrangências de aplicação, por consulta aos seguintes cadastros:

b.1) SICAF;

b.2) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/ceis>);

b.3) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php);

b.4) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>);

b.5) Lista de inidôneos mantida pelo Tribunal de Contas da União; e

b.6) módulo Registro de Ocorrências do SIGA.

c) por consulta ao SICAF, eventuais ocorrências impeditivas indiretas, hipótese na qual o gestor deverá verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

14.2.5.1. 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 as provas que pretende produzir. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CONTRATANTE.

14.2.5.2. 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.

14.2.5.3. 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.

14.2.5.4. 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.

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

14.2.6.1. 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.

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

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

14.2.7.2. 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.

14.2.8. 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% (meio por cento) ao mês, calculado pro rata die.

14.2.9. 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.

Do Reajuste:

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

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

Nos reajustes subsequentes ao primeiro, o interregno mínimo de 1 (um) ano será contado a partir da data do fato gerador que deu ensejo ao último reajuste.

Os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do ICTI - Índice de Custo da Tecnologia da Informação, exclusivamente para as obrigações que se iniciem após a anualidade, tendo em vista que o referido índice é o setorial indicado para contratações envolvendo TIC.

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

Fica a CONTRATADA obrigada 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.

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.

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.

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

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 da contratada, 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.

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

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

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

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.

REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio

Necessidade:

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.

Funcionalidades:

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

Requisitos de Capacitação

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.

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

A CONTRATADA deverá fornecer apostilas e vídeoaula contendo o material necessário a capacitação ofertada;

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.

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

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

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;

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

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

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

Os profissionais responsáveis por ministrar a capacitação deverão conhecer todos os aspectos técnicos e funcionais da solução aqui especificada, com experiência comprovada em capacitações no uso da solução.

A CONTRATADA será responsável pelas despesas relativas à participação de seus instrutores, tais como hospedagem, transporte, diárias, etc.

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.

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

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

Requisitos Legais

Aplicáveis ao Objeto:

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

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

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.

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.

Requisitos Temporais

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

Requisitos de Metodologia de Trabalho

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.

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

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

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

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.

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

Ordem de Fornecimento;

Ordem de Serviço;

Plano de Inserção;

Termos de Recebimento;

Chamado registrado na Central de Atendimento;

Ofícios;

Relatórios e Atas de Reunião;

E-mail; e

Demais Termos previstos no instrumento convocatório.

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.

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.

Indicação de marcas (ou modelos) e vedação de utilização de marca

Maiores detalhamentos e definições acerca da manutenção da marca ou de sua substituição serão evidenciados no item 17 deste Estudo Técnico durante o levantamento de soluções existentes no mercado, que revelará o cenário mais viável do ponto de vista técnico e econômico.

Requisitos de Sustentabilidade Ambiental

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.

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.

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 diretiva RoHS (Reduction of Hazardous Substances).

Requisitos Sociais e Culturais

Não se aplicam requisitos sociais e culturais para esta contratação.

De Arquitetura Tecnológica

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

De Projeto e da Implantação

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

Das atualizações do sistema

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.

Exigência de Credenciamento

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.

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.

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.

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

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

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.

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

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

Requisitos Materiais e Humanos

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.

Não será necessária a utilização de mão de obra especializada, tendo em vista que os recursos humanos necessários à instalação e configuração 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.

Necessidades de Adequações no Ambiente

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.

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

Reunião de kick-off

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

PREVISÃO E CONDIÇÕES DE PRESTAÇÃO DA GARANTIA CONTRATUAL

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:

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.

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.

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.

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.

Caso o prazo de vigência do contrato seja inferior a um ano, a garantia prevista no item 1 será calculada sobre o valor total do Contrato.

Na forma do art. 101 da Lei nº 14.133/2021, nos casos de contratos que impliquem a entrega de bens pela Administração, dos quais o contratado ficará depositário, o valor desses bens deverá ser acrescido ao valor da garantia.

O **contratado** poderá optar pelas seguintes modalidades de garantia:

caução em dinheiro ou em títulos da dívida pública;

seguro-garantia;

fiança bancária; e

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

Qualquer que seja a modalidade escolhida pelo **contratado**, a garantia assegurará o pagamento de:

prejuízos advindos do não cumprimento do objeto do Contrato e do não adimplemento das demais obrigações nestas previstas;

multas moratórias, compensatórias e administrativas aplicadas pela Administração ao **contratado**; e

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

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.

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.

Ressalvada a hipótese de seguro-garantia, em que deverá ser observado o prazo do item 16.10, 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 16.5.

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 apólice permanecerá em vigor mesmo que o **contratado** não pague o prêmio nas datas convenionadas;

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

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 16.8 deste Termo de Referência; e

a apólice somente será aceita se contemplar todos os eventos indicados no item 16.6, observada a legislação que rege a matéria.

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.

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 art. 827 do Código Civil.

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 16.21.

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 16.1 neste item.

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.

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.

O **contratante** executará a garantia na forma prevista na legislação que rege a matéria.

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.

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**.

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 nº 662, de 11 de abril de 2022.

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 do **contratante**, mediante termo circunstanciado, de que o **contratado** cumpriu todas as cláusulas do Contrato.

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 convenionado, em se tratando de extinção consensual da contratação.

O **contratado** autoriza o **contratante** a reter, a qualquer tempo, a garantia, na forma prevista no Edital e no Contrato.

No caso de inexecução total ou parcial do objeto, que acarrete a rescisão do Contrato, será automaticamente devida multa compensatória no valor de 5% (cinco por cento) do valor do Contrato.

INDICAÇÃO DE MARCAS E MODELOS OU VEDAÇÃO DE UTILIZAÇÃO DE MARCA/PRODUTO NA EXECUÇÃO DO SERVIÇO

Após análise apresentada no item "LEVANTAMENTO DE MERCADO" (item 5 do Estudo Técnico), optou-se pela escolha da marca, conforme motivos exposto abaixo:

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.

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 Estudo, é fundamentada em uma análise técnica e estratégica que visa garantir a máxima eficácia, escalabilidade, controle e conformidade para o ambiente da organização.

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.

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 dos Dados e 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.

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.

MODELO DE GESTÃO DO CONTRATO

Na forma do art. 4º do Decreto estadual nº 48.817/2023, a gestão e a fiscalização da execução da contratação serão realizadas por agentes públicos, designados pela autoridade do órgão ou entidade contratante, que indicará o gestor e fiscais para cada contrato, dentre os servidores lotados no órgão ou entidade, bem como seus substitutos, observando-se os requisitos estabelecidos na Lei nº 14.133/2021.

A gestão e a fiscalização da execução da contratação poderá ser realizada por uma Comissão de Gestão e Fiscalização, composta por, no mínimo, 3 (três) membros, integrada por gestor, fiscais e complementada conforme a necessidade pelos agentes definidos nos incisos I a III do art. 5º do Decreto acima referido, considerando a especificidade e complexidade do objeto ou da solução, de acordo com a necessidade e a critério da administração.

A Comissão de Gestão e Fiscalização anotará, em registro próprio, todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados.

A execução dos contratos deverá ser acompanhada e fiscalizada por meio de instrumentos de controle, definidos no art. 18 do Decreto estadual nº 48.817/2023.

Deve ser estabelecido, desde o início da execução contratual, mecanismo de controle da utilização dos materiais empregados nos contratos, para efeito de acompanhamento da execução do objeto bem como para subsidiar a estimativa para as futuras contratações.

O contratado declara, antecipadamente, aceitar todas as condições, métodos e processos de inspeção, verificação e controle adotados pela fiscalização, obrigando-se a fornecer todos os dados, elementos, explicações, esclarecimentos e comunicações de que esta necessitar e que forem julgados necessários ao desempenho de suas atividades.

A instituição e a atuação da fiscalização não exclui ou atenua a responsabilidade do contratado, nem a exime de manter fiscalização própria.

É vedada a atribuição ao contratado da avaliação de desempenho e qualidade da prestação dos serviços por ela realizada.

EXIGÊNCIAS DE HABILITAÇÃO JURÍDICA, TÉCNICA, FISCAL, SOCIAL E TRABALHISTA E ECONÔMICO-FINANCEIRA

Habilitação Jurídica

Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional.

Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede.

Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no [Portal do Empreendedor](#).

Sociedade Limitada Unipessoal - SLU: ato constitutivo, estatuto ou contrato social em vigor inscrito no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhado de documento comprobatório do administrador, sendo assim enquadrada a sociedade identificada como Empresas Individual de Responsabilidade Limitada – EIRELI, na forma do art. 41, da Lei nº 14.195, de 26 de agosto de 2021.

Sociedade Empresária Estrangeira em funcionamento no País: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020 ou norma posterior que regule a matéria.

Sociedade Simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores.

Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde se encontra estabelecida a matriz.

Sociedade Cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro de 1971, demonstrando que a sua constituição e funcionamento observam as regras estabelecidas na legislação aplicável, em especial a Lei nº 5.764/1971, a Lei nº 12.690, de 19 de julho de 2012, e a Lei Complementar nº 130, de 17 de abril de 2009.

Quando cabível, os documentos apresentados devem estar acompanhados de todas as alterações ou da consolidação respectiva

Habilitação Técnica

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:

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.

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.

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.

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

Será admitida, para fins de comprovação do 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.

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 executados os objetos.

Habilitação fiscal, Social e Trabalhista

Inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso.

Regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social.

Regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS).

Declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do art. 7º, XXXIII, da Constituição.

Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943.

Prova de inscrição no cadastro de contribuintes estadual/distrital e municipal, relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual

O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123/2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal, eis que a apresentação do Certificado de Condição de Microempreendedor Individual – CCMEI supre tais requisitos.

Prova de regularidade com a Fazenda do Estado do Rio de Janeiro, mediante a apresentação de:

Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, expedida pela Secretaria de Estado de Fazenda;

Certidão Negativa de Débitos em Dívida Ativa, ou Certidão Positiva com efeito de Negativa, para fins de participação em licitação, expedida pela Procuradoria Geral do Estado.

Regularidade com a Fazenda Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre, com a apresentação de Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, do imposto sobre serviços de qualquer natureza – ISS.

Regularidade com a Fazenda Estadual do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre, com a apresentação de Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, perante o Fisco estadual, pertinente ao Imposto sobre Operações relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual, Intermunicipal e de Comunicação – ICMS, bem como de Certidão perante a Dívida Ativa estadual, podendo ser apresentada Certidão Conjunta em que constem ambas as informações.

Caso o fornecedor seja considerado isento dos tributos municipais e/ou estaduais relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

Na hipótese de cuidar-se de microempresa ou de empresa de pequeno porte, na forma do art. 42 da Lei Complementar nº 123/2006, a documentação somente será exigida para efeito de assinatura do contrato, caso se sagre vencedora no certame.

Em sendo declarada vencedora do certame microempresa ou empresa de pequeno porte com débitos fiscais e trabalhistas, ficará assegurado, a partir de então, o prazo de 5 (cinco) dias úteis para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de negativas, na forma do art. 43, § 1º, da Lei Complementar nº 123/2006.

O prazo acima poderá ser prorrogado por igual período, a critério exclusivo da Administração Pública.

A não regularização da documentação no prazo estipulado implicará a decadência do direito à contratação, na forma do § 2º do art. 43 da Lei Complementar nº 123/2006, sem prejuízo de aplicação de sanções previstas no Edital.

Habilitação Econômico-Financeira

Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor, caso se trate de pessoa jurídica, ou certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do fornecedor, caso se trate de pessoa física ou de sociedade simples.

Não será causa de inabilitação do licitante a anotação de distribuição de processo de recuperação judicial ou de pedido de homologação de recuperação extrajudicial.

Balço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, vedada a sua substituição por balanços provisórios.

Os documentos referidos acima limitar-se-ão ao último exercício social no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

Os fornecedores criados no exercício financeiro da contratação deverão atender a todas as exigências da habilitação e ficam autorizados a substituir os demonstrativos contábeis pelo balanço de abertura;

Poderá ser apresentado o balanço intermediário, caso autorizado por lei ou pelo contrato/estatuto social. A exigência tem como objetivo assegurar que o licitante tenha condições de cumprir as obrigações contratuais, garantindo a qualidade e a execução do contrato.

Ao verificar a saúde financeira do licitante, a administração pública reduz o risco de inadimplência, atrasos e problemas na execução do contrato.

A apresentação do balanço patrimonial e das demonstrações contábeis contribui para a transparência do processo licitatório, permitindo que a administração pública avalie a situação financeira do licitante de forma mais precisa.

Caso o fornecedor seja cooperativa, o balanço e as demais demonstrações contábeis deverão ser acompanhados de cópia do parecer da última auditoria contábil-financeira, conforme dispõe o art. 112 da Lei nº 5.764/1971, ou de uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

Para fins de habilitação econômico-financeira de sociedade empresária em recuperação judicial deverão ser considerados os valores constantes no Plano de Recuperação Judicial, homologado pelo Juízo competente, para fins de apuração dos índices contábeis previstos no edital.

Comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), iguais ou superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

Caso seja apresentado resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverá ser comprovado capital ou patrimônio líquido mínimo de 1% (um por cento) do valor total estimado da contratação ou do item pertinente.

O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

OBRIGAÇÕES DA CONTRATANTE E CONTRATADA

Obrigações da CONTRATANTE:

- Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos neste Termo de Referência;
- Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, quando aplicável;
- Efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.
- Demais obrigações serão definidas no contrato e no edital.

Obrigações da CONTRATADA:

- Indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;
- Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;a;
- Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;
- Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;
- Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;
- Quando especificado, ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;
- Caso o fornecedor registrado ainda não tenha programa de integridade instituído, deverá implantar o Programa de Integridade no prazo de até 180 (cento e oitenta) dias corridos, a partir da assinatura do Contrato, na forma da legislação vigente.
- Demais obrigações serão definidas no contrato e no edital.

OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

I - Definições Gerais:

As partes, CONTRATANTE e CONTRATADO, deverão cumprir a Lei Federal nº 13.709/2018 (LGPD), e o Decreto Estadual nº 48.891/2024, que institui a Política de Governança em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro, quanto ao tratamento de dados pessoais em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

Para os fins da LGPD, na forma do seu art. 5º, incisos VI e VII, a CONTRATANTE corresponderá ao CONTROLADOR, enquanto a CONTRATADO corresponderá ao OPERADOR.

II - Critérios de tratamento de dados pessoais:

As partes, CONTRATANTE e CONTRATADO, deverão cumprir a Lei Federal nº 13.709/2018 (LGPD), e o Decreto Estadual nº 48.891/2024, que institui a Política de Governança em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro, quanto ao tratamento de dados pessoais em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

O CONTRATADO deve atender à Política de Segurança da Informação instituída pela Instrução Normativa do Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro (PRODERJ) nº 07 e demais normativos correlatos publicados pelo CONTRATANTE.

O tratamento de dados pessoais pelo CONTRATADO será limitado às atividades estritamente necessárias para o alcance das finalidades do objeto contratado ou, quando for o caso, ao cumprimento de obrigação legal ou regulatória, ao exercício regular de direito, por determinação judicial ou por requisição da Agência Nacional de Proteção de Dados.

O CONTRATADO somente poderá tratar os dados pessoais nos moldes expressamente definidos e em estrita consonância com as finalidades específicas delineadas pela CONTRATANTE, na forma dos Arts. 7º, 11, 14 e/ou 23 da Lei nº 13.709/2018.

O CONTRATADO deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que venha a ter conhecimento em razão da execução contratual.

O CONTRATADO deve assegurar que seus colaboradores e/ou prestadores de serviços que, no âmbito da execução contratual, venham a ter acesso a dados pessoais, cumpram as diretrizes protetivas de proteção aplicáveis, mediante a vinculação prévia a Termo de Sigilo e Confidencialidade.

É vedado ao CONTRATADO subcontratar, total ou parcialmente, o objeto do Contrato.

O CONTRATADO deverá manter sigilo absoluto sobre quaisquer dados ou informações contidas em documentos, mídias, meios de armazenamento ou canais de conectividade, sendo-lhe vedado, sob qualquer pretexto, divulgá-los, reproduzi-los ou utilizá-los, sob pena de lei.

É vedado às partes utilizar qualquer dado pessoal eventualmente repassado em decorrência da execução contratual para finalidade distinta daquela prevista no objeto, sob pena de responsabilização administrativa, civil e criminal.

As partes se comprometem a manter sigilo e confidencialidade de todas as informações — em especial dados pessoais e dados pessoais sensíveis — eventualmente repassados em decorrência da execução do contrato, em consonância com o disposto na Lei Federal nº 13.709/2018, sendo vedado o compartilhamento com terceiros, salvo hipóteses decorrentes de obrigações legais ou aquelas estritamente necessárias ao cumprimento do objeto contratual.

As partes responderão administrativa e judicialmente por eventuais danos patrimoniais, morais, individuais ou coletivos, causados aos titulares de dados pessoais, repassados em decorrência da execução contratual, por inobservância da Lei Geral de Proteção de Dados Pessoais (LGPD).

As partes comprometem-se a comunicar reciprocamente, no prazo máximo de 24 horas, qualquer incidente de segurança que envolva dados pessoais em decorrência do presente contrato — como acesso não autorizado, destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito, bem como a adotar as providências previstas no Art. 48 da LGPD.

PREVISÃO DE PERCENTUAL MÍNIMO DE MÃO DE OBRA RESPONSÁVEL PELA EXECUÇÃO DO OBJETO DA CONTRATAÇÃO CONSTITUÍDO POR MULHERES VÍTIMAS DE VIOLÊNCIA DOMÉSTICA

Em razão das características do objeto, não haverá contratação de mão de obra para a sua execução pelo que se entende não ser aplicável o disposto no art. 17, V, "f" do Decreto Estadual nº 48.816/2023 à execução destes serviços, o que não exime a empresa CONTRATADA de cumprir a reserva de cotas de que dispõe a Lei Estadual nº 7.382/2016, quando cabível.

MODALIDADE DE LICITAÇÃO, CRITÉRIO DE JULGAMENTO E MODO DE DISPUTA

O fornecedor será selecionado por meio da realização de procedimento licitatório, na modalidade PREGÃO, sob a forma ELETRÔNICA, com a adoção do critério de julgamento pelo MENOR PREÇO POR LOTE.

O modo de disputa será o ABERTO.

Em consonância ao inciso I do art. 56 da Lei Federal nº 14.133, de 2021 e atendimento ao art. 17, VI, “a” do Decreto Estadual nº 48.816/2023, no modo de disputa aberto, os licitantes apresentarão suas propostas por meio de lances públicos e sucessivos, crescentes ou decrescentes, visto que se trata de um pregão cujo critério de julgamento é menor preço por lote

Os preços em disputa aberta ficam claros aprimorando a competição entre os participantes e com isso reduzir riscos na contratação contribuindo para uma licitação que alcance mais prontamente os resultados pretendidos com a contratação.

Outrossim, não foi possível identificar que optar por modo disputa diferente do "modo aberto" venha a trazer vantagem para a Administração e nem mesmo aponta simplificação do processo ou celeridade no resultado da licitação.

PREVISÃO DA VEDAÇÃO OU DA PARTICIPAÇÃO DE EMPRESAS SOB A FORMA DE CONSÓRCIO NO PROCESSO DE CONTRATAÇÃO E JUSTIFICATIVA PARA O CASO DE VEDAÇÃO

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.

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.

PREVISÃO DA VEDAÇÃO OU DA PARTICIPAÇÃO DE COOPERATIVAS NO PROCESSO DE CONTRATAÇÃO E AO CASO DE VEDAÇÃO

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.”

PREVISÃO DA VEDAÇÃO OU DA POSSIBILIDADE DE SUBCONTRATAÇÃO, DO PERCENTUAL E DAS CONDIÇÕES

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.

ESTABELECIMENTO DE RESERVA DE COTA OU A EXCLUSIVIDADE DA LICITAÇÃO

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.

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.

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.

PRAZO DE VALIDADE E CONDIÇÕES DA PROPOSTA

Condições da proposta

O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

Valor unitário e total dos itens;

Marca;

Fabricante;

Descrição do objeto, contendo as informações similares à especificação deste Termo de Referência;

Quantidade cotada, que não poderá ser inferior ao quantitativo máximo de cada item que poderá ser adquirido.

Todas as especificações do objeto contidas na proposta vinculam o licitante.

O licitante não poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.

Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

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

Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional, conforme §1º do art. 17 da Lei Complementar 123/2006.

O licitante cujo estabelecimento esteja localizado no Estado do Rio de Janeiro deverá apresentar proposta isenta de ICMS, quando cabível, de acordo com o Convênio CONFAZ nº 26/2003 e a Resolução SEFAZ nº 971/2016, sendo este valor considerado para efeito de competição na licitação.

A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe este Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

Prazo de Validade

O prazo de validade da proposta não será inferior a 60 (sessenta) dias corridos, a contar da data de sua apresentação, podendo ser prorrogado, por igual período, salvo se houver justificativa para prazo diverso aceita pela Administração.

Os licitantes devem respeitar os preços máximos estabelecidos no Anexo do Edital referente ao orçamento estimado (art. 59, III, da Lei nº 14.133/2021).

Os licitantes devem respeitar os preços unitários máximos estabelecidos no Anexo do Edital para os itens que compõem o lote, se for o caso.

O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas do Estado e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

REGRAS PARA INSPEÇÃO DE AMOSTRA, PROVA DE CONCEITO OU EXAME DE CONFORMIDADE

Prova de Conceito:

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

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.

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.

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.

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.

A prova de conceito consistirá na apresentação do funcionamento do objeto, conforme especificações constantes do Anexo I - Especificações Técnicas do Objeto ([127236377](#)).

CRITÉRIOS DE DESEMPATE COM BASE NO DESENVOLVIMENTO PELO LICITANTE DE AÇÕES DE EQUIDADE ENTRE HOMENS E MULHERES NO AMBIENTE DE TRABALHO

O desenvolvimento, pelo licitante, de ações de equidade entre mulheres e homens no ambiente de trabalho será critério de desempate no processo licitatório, conforme dispõem o art. 60, inciso III da Lei nº 14.133/2021, o art. 30 do Decreto nº 48.778/2023 e o art. 10 do Decreto nº 49.233/2024 que regulamentou a matéria no âmbito estadual.

Na forma disposta no art. 10, § 1º do referido normativo estadual, serão consideradas ações de equidade, respeitada a seguinte ordem:

medidas de recrutamento igualitário entre mulheres e homens;

igualdade de remuneração e paridade salarial entre mulheres e homens;

plano de carreira desenvolvido com expressa menção à ascensão profissional igualitária entre mulheres e homens, inclusive previsão de participação proporcional no quadro diretor da empresa;

estabelecimento de canal de denúncia e garantia de apuração de práticas de assédio moral e sexual, inclusive com a implementação de políticas de tolerância zero com relação a todas as formas de violência no trabalho, incluindo abuso verbal e/ou físico;

ações em saúde e segurança do trabalho que considerem as diferenças entre os gêneros;

investimentos na capacitação de mulheres para o exercício gerencial;

promoção de programas educativos de gerentes e chefes de setores que possibilitem o reconhecimento de sinais de violência no ambiente de trabalho;

provisão de sala de apoio à amamentação com vistas a uma cultura de respeito e apoio à amamentação como forma de promover a saúde da mulher trabalhadora e de seu bebê, no caso de empresas que possuam em seus quadros mais de 30 (trinta) mulheres com idade superior a 16 (dezesesseis) anos, quantitativo previsto no art. 389, § 1º, do Decreto-Lei nº 5.452/1943 (Consolidação das Leis do Trabalho), de acordo com a estratégia "Apoio à Mulher Trabalhadora que Amamenta" do Ministério da Saúde e da Secretaria de Estado de Saúde; e

adesão ao "Programa Empresa Cidadã", instituído pela Lei nº 11.770/2008, regulamentado pelos arts. 137 a 142 do Decreto nº 10.854/2021, destinados à prorrogação das licenças-maternidade e paternidade, mediante incentivo fiscal.

O licitante que atender, a pelo menos 2 (dois) dos incisos do § 1º do art. 10 (acima transcrito), terá sua proposta enquadrada no art. 60, inciso III da Lei nº 14.133/2021, **para efeito de desempate**, observado o disposto no § 5º do art. 42 do Decreto nº 48.778/2023.

O licitante que possuir o selo Empresa Amiga da Mulher, conferido nos termos da Lei nº 9.173/2021 e da Lei nº 14.682/2023 ou o selo Empresa Amiga da Amamentação, conferido pela Lei nº 14.683/2023 ficará dispensado da comprovação do desenvolvimento das ações de equidade de que trata o § 1º do art. 10 do Decreto estadual nº 49.233/2024.

CRITÉRIOS DE DESEMPATE COM BASE NO ART. 60 DA LEI Nº 14.133/2021

Em caso de eventual empate entre propostas ou lances, serão utilizados os seguintes critérios de desempate, nesta ordem, conforme regulamentação do Decreto estadual nº 48.778/2023:

contratação de microempresas e empresas de pequeno porte, nos termos dos arts. 44 e 45 da Lei Complementar nº 123/2006, observado o disposto no art. 4º da Lei nº 14.133/2021;

disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos na Lei;

desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme Decreto nº 49.233/2024;

desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

empresas brasileiras;

empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

JUSTIFICATIVA PARA ESCOLHA DO SISTEMA DE REGISTRO DE PREÇOS

De acordo com o art. 3º do Decreto 48.843/23, o SRP deverá ser adotado, preferencialmente, nas seguintes hipóteses:

quando a contratação se voltar ao atendimento de necessidade permanente, prolongada ou frequente do bem ou do serviço a ser contratado;

quando for mais conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, por quantidade de horas de serviço ou postos de trabalho, ou em regime de tarefa;

quando for conveniente para atendimento a mais de um órgão ou entidade, bem como aos programas de governo; ou
quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

O Governo do Estado, como toda grande organização, tem gastos volumosos com produtos e serviços de Tecnologia da Informação e Comunicação (TIC) entre os órgãos que o compõe. Os crescentes desafios colocados para o governo acabam induzindo o aumento da máquina administrativa e, conseqüentemente, dos gastos com seus serviços. Desta forma, entendemos que o registro de preços se justifica, especialmente no que tange aos incisos I e III do referido Decreto.

Parte significativa desses dispêndios pode ser reduzida com processos de contratações eficientes, planejados previamente em conjunto por grupos de Órgãos. Além de melhorar a qualidade técnica dos artefatos de contratação, um planejamento integrado de contratação reduz a duplicidade de esforços entre os órgãos e otimiza o trabalho dos técnicos das áreas de licitações e contratos, ensejando ainda economia processual.

O grande benefício, entretanto, advém da utilização do poder de compra do governo. Na medida em que aproveita as oportunidades de economia de escala, a Administração Pública pode obter melhores preços junto ao mercado, reduzindo seus custos em benefício do atendimento às demandas sociais.

Esta é uma inteligência trazida pelo Sistema de Registro de Preços - SRP, utilizado sempre que conveniente à contratação de serviços para atendimento a vários Órgãos, que trabalham de forma integrada com suas estimativas de consumo e os aspectos técnicos da contratação.

Em suma, elencamos alguns argumentos que justificam a adoção do Sistema de Registro de Preços:

Melhoria da qualidade técnica dos documentos preliminares ao certame, tais como: especificações técnicas, alinhamento estratégico com o planejamento dos órgãos e condições jurídicas para a contratação;

Redução do esforço administrativo para a realização de diversos processos licitatórios sendo que a execução conjunta culmina em um único certame;

Redução de custos de manutenção e melhor eficiência pelo uso racional dos recursos, uma vez que estes foram definidos de forma a atender precisamente as necessidades do usuário;

Ganho de economia de escala, pois, ao prospectar grandes volumes licitados, a Administração Pública amplia seu poder de compra junto aos fornecedores e consegue reduções consideráveis de preços, fato que certamente não ocorreria quando do fracionamento de certames.

Portanto, a utilização do Sistema de Registro de Preços será necessária neste certame, uma vez que atenderá as demandas do PRODERJ e demais órgãos da Administração Pública, podendo o quantitativo ora definido sofrer alterações, assim como está voltada para o atendimento de necessidade permanente, prolongada ou frequente do serviço.

INDICAÇÃO DO ÓRGÃO OU ENTIDADE GERENCIADOR DA ATA

Compete ao nível de Direção Geral, representado pelo PRODERJ, conduzir e disponibilizar, mas não limitado, atas de registro de preços, contratos e contratos corporativos para suprir itens relativos à TIC aos órgãos da administração pública de acordo com as políticas e diretrizes estabelecidas, tendo como objetivo a obtenção de ganhos e economia de escala para o Estado, além de benefícios intrínsecos de padronização e integração, conforme determina o inciso XIII, art. 3º do Decreto Estadual 48.997/2024.

Desta forma, o PRODERJ será o órgão Gerenciador.

INDICAÇÃO DOS ÓRGÃOS OU ENTIDADES PARTICIPANTES DA ATA

Após a realização de Intenção de Registro de Preços - IRP, os seguintes órgãos, além do PRODERJ, manifestaram pretensão de participar da licitação:

OBRIGAÇÕES DO ÓRGÃO GERENCIADOR DA ATA

São atribuições do gerenciador:

- aferir, semestralmente, a compatibilidade dos preços registrados com os efetivamente praticados;
- divulgar os preços registrados e suas atualizações no Portal de Compras do Estado do Rio de Janeiro;
- praticar todos os atos de controle e gerenciamento dos quantitativos das Atas de Registro de Preços e de seus saldos, das solicitações de adesão e do remanejamento das quantidades;
- gerenciar a Ata de Registro de Preços, providenciando a indicação, sempre que solicitado, dos fornecedores registrados para atendimento às necessidades do órgão ou entidade, obedecendo à ordem de classificação do certame e os quantitativos de contratação definidos pelos participantes da ata;
- deliberar quanto à adesão posterior de órgãos e entidades que não manifestaram interesse em participar do registro de preços durante o período de divulgação da Intenção de Registro de Preços;
- convocar os proponentes remanescentes, nas hipóteses autorizadas pela Ata e pelo Decreto nº 48.843/2023, observada a ordem de classificação;
- conduzir as alterações ou as atualizações dos preços registrados; e
- promover a correta gestão, fiscalização e execução contratual, nos termos do Capítulo VI do Título III da Lei nº 14.133/2021, do disposto no Decreto nº 48.817/2023, no presente Termo de Referência e no contrato, com relação às suas próprias contratações.

OBRIGAÇÕES DA BENEFICIÁRIA DA ATA

São atribuições dos participantes:

- auxiliar tecnicamente, por solicitação do gerenciador, as atividades previstas nos incisos VIII, IX e XI do *caput* do art. 6º do Decreto nº 48.843/2023;
- tomar conhecimento da Ata de Registro de Preços, inclusive de eventuais alterações, para o correto cumprimento de suas disposições;
- prestar informações, quando solicitadas, ao gerenciador quanto à contratação e à execução da demanda destinada ao seu órgão ou entidade;
- informar ao gerenciador a eventual recusa do contratado em atender às condições estabelecidas no instrumento convocatório, quando houver, e no presente Termo de Referência, firmadas na Ata de Registro de Preços, bem como as divergências relativas à entrega, características e origem dos bens adjudicados; e
- promover a correta gestão, fiscalização e execução contratual, nos termos do Capítulo VI do Título III da Lei nº 14.133/2021, e o disposto no Decreto nº 48.817/2023, no presente Termo de Referência e no contrato, com relação às suas próprias contratações.

OBRIGAÇÕES DOS ÓRGÃOS NÃO-PARTICIPANTES

São atribuições dos não-participantes:

- aceitar todas as condições fixadas na Ata de Registro de Preços;
- tomar conhecimento da Ata de Registro de Preços, inclusive de eventuais alterações, para o correto cumprimento de suas disposições;
- prestar informações, quando solicitadas, ao gerenciador quanto à contratação e à execução da demanda destinada ao seu órgão ou entidade;
- informar ao gerenciador a eventual recusa do contratado em atender às condições estabelecidas no instrumento convocatório, quando houver, e no presente Termo de Referência, firmadas na Ata de Registro de Preços, bem como as divergências relativas à entrega, características e origem dos bens adjudicados; e
- promover a correta gestão, fiscalização e execução contratual, nos termos do Capítulo VI do Título III da Lei nº 14.133/2021, e o disposto no Decreto nº 48.817/2023, no presente Termo de Referência e no contrato, com relação às suas próprias contratações.

ESTIMATIVA TOTAL DE QUANTIDADES DA CONTRATAÇÃO

As contratações adicionais pelos não-participantes não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens registrados na Ata de Registro de Preços para o gerenciador e para os participantes, quando houver.

O quantitativo decorrente das adesões à Ata de Registro de Preços não poderá exceder, na totalidade, ao limite de 200% (duzentos por cento) do quantitativo de cada item registrado na Ata para o gerenciador e para os participantes, quando houver, independentemente do número de órgãos ou entidades não-participantes que aderirem.

É vedada a participação do órgão ou da entidade em mais de uma Ata de Registro de Preços com o mesmo objeto no prazo de validade daquela de que já tiver participado, salvo na ocorrência de ata que tenha registrado quantitativo inferior ao máximo previsto no edital da licitação.

Indicação dos órgãos participantes conforme IRP

ÓRGÃOS PARTICIPANTES
PRODERJ
RIOPREVIDÊNCIA
FAF

Previsão de contratação pelo gerenciador e pelos participantes conforme IRP

LOTE I					
Item	Código ID SIGA	Descrição	Métrica	Forma de Fornecimento	Quantidade
1	195087	Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, com Instalação da Solução.	UN	Aquisição	3
2	195079	Serviço técnico especializado de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação	UST	Sob Demanda	3000
3	195078	Treinamento da Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	Turma	Sob Demanda	3

LOTE II					
Item	Código ID SIGA	Descrição	Métrica	Forma de Fornecimento	Quantidade
4	196478	Equipamento para a interceptação do tráfego	UN	Aquisição de Equipamento	3
5	195071	Licenciamento de deduplicação do tráfego.	UN	Subscrição de Licença por 36 meses	3
6	195072	Licenciamento avançado de descrição do tráfego.	UN	Subscrição de Licença por 36 meses	3
7	195073	Licenciamento avançado de análise de aplicações.	UN	Subscrição de Licença por 36 meses	3
8	195074	Licenciamento avançado de análise de metadados.	UN	Subscrição de Licença por 36 meses	3
9	193207	Módulo de expansão do processamento.	UN	Aquisição de Equipamento	2
10	123672	Módulo de expansão para a captura do tráfego "inline".	UN	Aquisição de Equipamento	3
11	195075	Licenciamento para o gerenciamento centralizado da solução.	UN	Subscrição de Licença por 36 meses	3
12	195076	Interceptador do tráfego virtualizado avançado.	UN	Subscrição de Licença por 36 meses	3
13	196651	Chassi para interconector passivo de interceptação do tráfego - interfaces ópticas	UN	Aquisição de Equipamento	3
14	196668	Interconector passivo de interceptação do tráfego – interfaces SFP	UN	Aquisição de Equipamento	3
15	196641	Interconector passivo de interceptação do tráfego – interfaces QSFP	UN	Aquisição de Equipamento	3
16	196667	Interconector passivo de interceptação do tráfego – interfaces RJ-45	UN	Aquisição de Equipamento	3
17	196499	Concentrador de Tráfego de Segurança.	UN	Aquisição de Equipamento	3

18	195083	Transceiver tipo 1 – 1 Gbps ethernet	UN	Aquisição de Equipamento	16
19	195084	Transceiver tipo 2 – 10 Gbps ethernet	UN	Aquisição de Equipamento	16
20	195085	Transceiver tipo 3 – 25 Gbps ethernet	UN	Aquisição de Equipamento	16
21	195086	Transceiver tipo 4 – 100 Gbps ethernet	UN	Aquisição de Equipamento	16
22	196666	Serviço técnico especializado para a solução de interceptação de tráfego.	UN	Sob Demanda	6022

LOTE III					
Item	Código ID SIGA	Descrição	Métrica	Forma de Fornecimento	Quantidade
23	195077	Licenciamento Elastic Enterprise On-Premises	UN	Subscrição de Licença por 36 meses	18
24	195080	Serviço técnico especializado para o Licenciamento Elastic Enterprise On-Premises.	UST	Sob Demanda	5596

Previsão de contratação pelos não-participantes

PARÂMETRO	LOTE I			LOTE II																		LOTE III		
	Item 01	Item 02	Item 03	Item 04	Item 05	Item 06	Item 07	Item 08	Item 09	Item 10	Item 11	Item 12	Item 13	Item 14	Item 15	Item 16	Item 17	Item 18	Item 19	Item 20	Item 21	Item 22	Item 23	Item 24
Quantidade máxima de contratação por meio de adesão (dobro da estimativa por item)	6	6.000	6	6	6	6	6	6	4	6	6	6	6	6	6	6	6	32	32	32	32	12.044	36	11.192
Quantidade máxima de contratação por órgão aderente (metade da estimativa por item)	2	1.500	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	8	8	8	8	3.011	9	2.798

ESTIMATIVA DO VALOR DA CONTRATAÇÃO

O custo estimado da contratação, após pesquisa de preços, é de **R\$ 95.053.904,70 (noventa e cinco milhões, cinquenta e três mil novecentos e quatro reais e setenta centavos)**, de acordo com pesquisa elaborada com base nos requisitos dos arts. 28 a 32 do do Decreto estadual nº 48.816/2023, que constará em documento anexo, separado e classificado conforme permissivo do mesmo normativo (art. 17, VIII).

O preço unitário de cada item, após pesquisa de preços, considerando as respectivas quantidades definidas na Intenção de Registro de Preços, é:

LOTE I								
ITEM	ID SIGA	ID PCA	DESCRIÇÃO	MÉTRICA	QUANTIDADE	FORMA DE FORNECIMENTO	PREÇO UNITÁRIO	TOTAL POR ITEM
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	3	Aquisição	R\$ 2.600.000,0000	R\$ 7.800,00,0000

2	195079	15932	Serviço técnico especializado de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	UST	3000	Sob Demanda	R\$ 590,0000	R\$ 1.770.000,0000
3	195078	15931	Treinamento da Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	Turma	3	Sob Demanda	R\$ 141.000,0000	R\$ 423.000,0000

TOTAL ESTIMADO DO LOTE I: R\$ 9.993.000,0000

LOTE II

ITEM	ID SIGA	ID PCA	DESCRIÇÃO	MÉTRICA	QUANTIDADE	FORMA DE FORNECIMENTO	PREÇO UNITÁRIO	TOTAL POR ITEM
4	196478	15936	Equipamento para a interceptação do tráfego	Unidade	3	Aquisição de Equipamento	R\$ 4.312.064,4700	R\$ 12.936.193,4100
5	195071	15921	Licenciamento de desduplicação do tráfego.	Unidade	3	Subscrição de Licença por 36 meses	R\$ 996.062,9400	R\$ 2.988.188,8200
6	195072	15923	Licenciamento avançado de descriptação do tráfego.	Unidade	3	Subscrição de Licença por 36 meses	R\$ 894.553,9300	R\$ 2.683.661,7900
7	195073	15927	Licenciamento avançado de análise de aplicações.	Unidade	3	Subscrição de Licença por 36 meses	R\$ 885.953,2400	R\$ 2.657.859,7200
8	195074	15935	Licenciamento avançado de análise de análise de metadados.	Unidade	3	Subscrição de Licença por 36 meses	R\$ 891.864,9800	R\$ 2.675.594,9400
9	193207	15937	Módulo de expansão do processamento.	Unidade	2	Aquisição de Equipamento	R\$ 938.923,8550	R\$ 1.887.847,7100
10	123672	15933	Módulo de expansão para a captura do tráfego "inline".	Unidade	3	Aquisição de Equipamento	R\$ 1.089.549,8000	R\$ 3.268.649,4000
11	195075	15924	Licenciamento para o gerenciamento centralizado da solução.	Unidade	3	Subscrição de Licença por 36 meses	R\$ 366.379,7900	R\$ 1.099.139,3700
12	195076	15938	Interceptor do tráfego virtualizado avançado.	Unidade	3	Subscrição de Licença por 36 meses	R\$ 4.289.807,9000	R\$ 12.869.423,7000
13	196651	15919	Chassi para interconector passivo de interceptação do tráfego - interfaces ópticas	Unidade	3	Aquisição de Equipamento	R\$ 13.468,6300	R\$ 40.405,8900
14	196668	15928	Interconector passivo de interceptação do tráfego – interfaces SFP	Unidade	3	Aquisição de Equipamento	R\$ 174.094,7700	R\$ 522.284,3100
15	196641	15925	Interconector passivo de interceptação do tráfego – interfaces QSFP	Unidade	3	Aquisição de Equipamento	R\$ 293.450,1300	R\$ 880.350,3900
16	196667	15916	Interconector passivo de interceptação do tráfego – interfaces RJ-45	Unidade	3	Aquisição de Equipamento	R\$ 345.534,9400	R\$ 1.036.604,8200
17	196499	15922	Concentrador de Tráfego de Segurança.	Unidade	3	Aquisição de Equipamento	R\$ 1.180.250,3200	R\$ 3.540.750,9600
18	195083	15915	Transceiver tipo 1 – 1 Gbps ethernet	Unidade	16	Aquisição de Equipamento	R\$ 3.579,5500	R\$ 57.272,8000
19	195084	15934	Transceiver tipo 2 – 10 Gbps ethernet	Unidade	16	Aquisição de Equipamento	R\$ 13.696,9700	R\$ 219.151,5200
20	195085	15926	Transceiver tipo 3 – 25 Gbps ethernet	Unidade	16	Aquisição de Equipamento	R\$ 14.301,8000	R\$ 228.828,8000
21	195086	15930	Transceiver tipo 4 – 100 Gbps ethernet	Unidade	16	Aquisição de Equipamento	R\$ 52.198,8100	R\$ 835.180,9600
22	196666	15929	Serviço técnico especializado para a solução de interceptação de tráfego.	UST	6022	Sob Demanda	R\$ 933,7000	R\$ 5.622.741,4000

TOTAL ESTIMADO DO LOTE II: R\$ 56.040.130,7100

LOTE III

ITEM	ID SIGA	ID PCA	DESCRIÇÃO	MÉTRICA	QUANTIDADE	FORMA DE FORNECIMENTO	PREÇO UNITÁRIO	TOTAL POR ITEM
23	195077	15917	Licenciamento Elastic Enterprise On-Premises.	Unidade	18	Subscrição de Licença por 36 meses	R\$ 1.314.198,9450	R\$ 23.655.581,0100
24	195080	15920	Serviço técnico especializado para o Licenciamento Elastic Enterprise On-Premises.	UST	5596	Sob Demanda	R\$ 958,7550	R\$ 5.365.192,9800

TOTAL ESTIMADO DO LOTE III: R\$ 29.020.773,99

MATRIZ DE ALOCAÇÃO DE RISCOS

O mapa de riscos, parte integrante e indissociável do Estudo Técnico Preliminar, identificou, avaliou e tratou os riscos inerentes à contratação, com definição de probabilidade, impacto, ações preventivas e de contingência e responsáveis, ao longo das fases preparatória, de seleção do fornecedor e de gestão do contrato. Considerando que a contratação não envolve alocação objetiva de riscos com efeitos sobre o equilíbrio econômico-financeiro nem transferência contratual de riscos ao particular, não se aplica a adoção de matriz de riscos, sendo o mapa de riscos suficiente para o adequado planejamento e gestão do ajuste. Ademais, por se tratar de registro de preços, s.m.j., os riscos já estarão contingenciados na Ata de Registro de Preços, prescindindo a apresentação da matriz de riscos.

NECESSIDADE DE REALIZAÇÃO DE AUDIÊNCIA PÚBLICA

A realização de audiência é dispensável tendo em vista que a pesquisa de mercado elaborada com base nos requisitos dos arts. 28 a 32 do Decreto Estadual nº 48.816/2023 não apurou valor estimado de grande vulto, na forma do art. 54, §2º do mesmo Decreto.

DISPOSIÇÕES FINAIS

O presente termo de referência foi concebido com base nas normas legais aplicadas à matéria e nas premissas recomendadas pelo Tribunal de Contas do Estado do Rio de Janeiro – TCE/RJ e a Procuradoria-Geral do Estado - PGE/RJ. Este documento constituirá parte integrante do edital da licitação a ser instaurado para viabilizar a contratação de empresa devidamente qualificada e que apresente o melhor preço para fornecimento dos serviços objeto desta demanda.

As empresas interessadas em participar da licitação serão integralmente responsáveis pela avaliação e levantamento dos custos relativos à execução do objeto, sendo inteiramente responsáveis por eventuais prejuízos decorrentes de avaliação equivocada ou da sua ausência.

Observadas as disposições da Lei Federal nº 12.527/2011 e do Decreto Estadual nº 46.475/2018, que tratam do direito e das restrições de acesso às informações sob guarda do poder público, fica registrado que o presente documento, assim como os seus anexos, são de acesso PÚBLICO.

ANEXOS

Abaixo, estão listados os documentos anexos cujas disposições estão em plena concordância com este Termo de Referência, do qual correspondem a parte integrante e indissociável:

Especificações Técnicas do Objeto ([128113619](#));

Catálogo de Serviços ([128114483](#));

Prova de Conceito I ([128113717](#));

Prova de Conceito II ([128113416](#));

Modelo de Relatório de Cumprimento do Objeto ([128113815](#));

Modelo de Termo de Confidencialidade e Sigilo ([128115013](#));

Modelo de Ordem de Serviço / Fornecimento ([128113942](#));

Modelo de Planilha de Composição de Preços ([128115139](#));

Modelo de Termo de Recebimento Provisório ([128115550](#)); e

Modelo de Termo de Recebimento Definitivo ([128116073](#)).

EQUIPE RESPONSÁVEL

RESPONSÁVEL PELA REVISÃO

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 Araújo, 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 **128113277** e o código CRC **EA48800F**.



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 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 detecção 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 análise de incidentes baseado em IA ou execução de machine learning no core central da solução sem necessidade de análise 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 autônoma baseado em IA sem uso de assinaturas já 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 IPs 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 ameaças 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 correlacionamento 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 detecção 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 detecção 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 (projektor, 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 tráfego 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 (dezesesseis) 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 cascadeamento (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 cascadeamento/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 módulo.

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 descryptografia 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 decryptado 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 descryptografia 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 descryptografados, 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 descryptografia 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 permitir 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. **CARACTERÍSTICAS 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 promiscuo 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 containerização (Kubernetes) através de Container TAPs.

1.41.10. Deverá coletar o tráfego no ambiente de containerização 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 decríptação, eliminando a necessidade de posicionamento de soluções de decríptação 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 containerização, 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 decifração passiva (out-of-band) do tráfego TLS.
 - 1.42.9.1. Deve implementar a captura de pacotes antes da criptografia e após a decifração, no mínimo para os seguintes sistemas operacionais e ambientes de containerização:

- 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 INTERCONNECTOR 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 0°C a 60°C 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”, “híbrida”, “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 (dezesesseis) 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 necessidade 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 realizar, 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 14:15, 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 **128113619** e o código CRC **283EDBEA**.

Referência: Processo nº SEI-430002/001505/2024

SEI nº 128113619

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:



ANEXO II

CATLOGO DE SERVIOS

1. CATLOGO DE SERVIOS REFERENTES  UNIDADE DE SERVIO TCNICO – UST

1.1. O catlogo de servios estabelece as atividades dentro de cada fase da Soluão de interceptaão de trfego, monitoramento de comportamento anmalo da rede, detecão, anlise e resposta de incidentes de segurana da informaão, incluindo hardware, software e demais componentes, bem como treinamento e garantia com manutenão do fabricante por 36 (trinta e seis) meses. As Ordens de Servio para execuão dos projetos sero realizadas a partir do consumo de UST dos itens do catlogo.

1.2. Os servios tcnicos especializados relativos aos sistemas e suporte a soluões de automaão com atendimento remoto e on-site (no local), sero realizados sob demanda, a partir de um conjunto de atividades estabelecido no Catlogo de Servios, aqui apresentado, em consonncia com as etapas previstas no planejamento de execuão dos projetos, e estabelece uma sequncia de atividades que podem ser aplicadas no desenvolvimento de cada projeto, bem como, da complexidade tpica esperada na realizaão das atividades preconizadas.

1.3. Os servios tcnicos especializados tero como unidade de medida a “unidade de servio tcnico” (UST) e sero requisitados, sob demanda, por meio de ordem de servio.

1.4. O modelo de quantificaão por UST  baseado na quantificaão detalhada de cada esforo de trabalho realizado para obtenão dos servios necessrios no escopo deste Estudo Tcnico Preliminar.

1.5. A fim de uniformizar o entendimento sobre os termos utilizados, seguem algumas definiões:

- Unidade de Servio Tcnico – UST: mtrica utilizada para aferir o custo de cada atividade a ser desempenhada;
- Custo em UST – representa o custo de cada atividade, considerando o tempo de duraão em UST e o peso de cada UST; e
- Duraão em UST – Tempo de duraão para execuão de cada atividade, considerando que uma UST tem a duraão 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 SERVIO TCNICO	
Complexidade	Fator de Ajuste
Baixa	1,00
Mdia	1,25
Alta	1,50

Lote I - Item 2 - Do Quantitativo de Servios e Memria de clculo - UST

Atividade	Complexidade (Baixa, Mdia ou Alta)	Tipo de Execuão (Remota ou Presencial)	Duraão do Servio (horas)	Validaão dos Servios Executados (horas)	Documentaão dos Servios 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 trfego e proteão de rede	MDIA	PRESENCIAL	18	6	8	32	40	1	40
Levantamento de requisitos de proteão automatizada	MDIA	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	MDIA	PRESENCIAL	26	6	12	44	55	3	165
Configuraão fsica no rack (energia, cabeamento, rede de gesto)	MDIA	PRESENCIAL	24	6	12	42	53	1	53
Configuraão da Soluão de Gerenciamento Centralizado	MDIA	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 Perfis 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 perfis 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 Serviços Executados (horas)	Documentação dos Serviços Executados (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 Gerenciamento Centralizado	ALTA	PRESENCIAL	8	1	8	17	25	2	34
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 (Firewall, IDS/IPS, SIEM, EDR ou NDR)	ALTA	REMOTO	48	1	3	52	78	2	104
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 latência	MEDIA	REMOTO	4	1	3	8	10	2	16
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 decriptografia 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 Serviços Executados (horas)	Documentação dos Serviços Executados (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 externo (Zabbix, Prometheus, etc.)	ALTA	REMOTO	16	10	8	34	51	2	102
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 CPU/memória	BAIXA	REMOTO	15	1	1	17	17	3	51
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 14:15, 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 **128114483** e o código CRC **D6829524**.

Referência: Processo nº SEI-430002/001505/2024

SEI nº 128114483

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 III - PROVA DE CONCEITO I

INTRODUÇÃO

A prova de conceito consistirá na apresentação do funcionamento dos Serviços de Fábrica de Teste, Qualidade e Métricas.

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":

Disponibilização de máquinas virtuais e/ou estações de trabalho, projetor e link de internet;

Criação de VLAN's e/ou disponibilização de endereços IP e entrada de DNS;

Criação de servidores de aplicação web;

Criação de usuários no AD e/ou modificações de regras de firewall, IPS, etc;

Caso seja aplicável, a disponibilização de periféricos, tais como: cabos, switches e outros componentes semelhantes não mencionados.

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:

ID do requisito;

Descrição do requisito;

Nome do produto ofertado (modelo, marca e fabricante);

Nome do documento de referência onde é possível verificar evidência do atendimento do requisito;

Página do documento referência onde é possível verificar evidência do atendimento do requisito;

Outras informações necessárias.

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.

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.

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.

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.

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.

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.

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.

A prova de conceito (POC) deve ser precedida em horário comercial, das 9h às 12h e das 14h às 18h.

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.

A prova será realizada no ambiente do PRODERJ, a ser definido no ato da convocação em um dos endereços abaixo mencionados:

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;

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

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	NA O
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 registrar 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 detecção, 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	Audidores (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 tráfego 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 de 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 14:16, 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 **Luis 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 **128113717** e o código CRC **708FDC63**.



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 PRODERTJ 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 requirite 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 técnico 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 14:16, 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 **128113416** e o código CRC **FA0A6B4E**.

Referência: Processo nº SEI-430002/001505/2024

SEI nº 128113416

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 V

MODELO DE RELATÓRIO DE CUMPRIMENTO DO OBJETO

obs: Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

(logo da empresa)

1. IDENTIFICAÇÃO			
Contrato nº			
Contratada		CNPJ	
nº da OS/OF		Período de Referência	

2. ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES DE ENTREGA/EXECUÇÃO					
Descrição do Objeto Contratado					
Item / Lote	Descrição do bem ou serviço	Métrica	Quantidade	Valor Unitário	Valor Total
Valor Total					

3. OBSERVAÇÕES

4. ENCAMINHAMENTO

Por este instrumento, encaminhamos as informações e documentos comprobatórios dos serviços correspondentes à [Ordem de Serviço ou de Fornecimento] acima identificada, conforme definido no Modelo de Execução do contrato supracitado, para que seja verificado o devido cumprimento dos requisitos e demais condições contratuais

5. PREPOSTO

Nome
CPF

Local e Data

Rio de Janeiro, na data da assinatura eletrônica.



Documento assinado eletronicamente por **Rodolfo Targino de Araujo, Assistente**, em 23/03/2026, às 14:16, 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 **128113815** e o código CRC **14119037**.

Referência: Processo nº SEI-430002/001505/2024

SEI nº 128113815

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 VI

MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO

este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

ANEXO XXX - DO CONTRATO

MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO

Eu, <nome completo>, <ocupação institucional>, <órgão público / entidade>, <matrícula>, <CPF>, declaro a ciência das obrigações e responsabilidades decorrentes do tratamento de dados pessoais realizado durante a vigência contratual, observando o integral teor do presente Termo de Responsabilidade.

Considerando as obrigações a mim conferidas, no bojo deste Termo de Responsabilidade, comprometo-me a:

- a) manusear as bases de dados com objetivo exclusivo de alcançar a finalidade específica atrelada ao tratamento dos dados pessoais envolvidos;
- b) não compartilhar com terceiros os dados pessoais sujeitos a qualquer espécie de tratamento, salvo se por meio oficial e quando estritamente necessário à concretização das atribuições;
- c) manter a absoluta cautela quando da exibição de dados pessoais em tela, por meio de impressões, ou, ainda, na gravação em meios eletrônicos, com escopo de inibir o acesso de terceiros não autorizados;
- d) não me ausentar do terminal sem encerrar a sessão de uso das bases, inibindo a prática de ações virtuais por terceiros não autorizados;
- e) não armazenar documentos de natureza particular em pastas institucionais;
- f) manter o sigilo dos dados pessoais ou informações sigilosas obtidas por força de minhas atribuições, mediante abstenção de compartilhamento e/ou divulgação a terceiros, sob pena de incorrer em sanções administrativas, civis e/ou penais decorrentes de eventual violação; e
- g) comunicar imediatamente ao Encarregado pelo tratamento de dados pessoais a ocorrência de qualquer ação ou omissão que contrarie o disposto neste termo, pelos meios formais disponibilizados pela instituição.

Rio de Janeiro, XX de XXXXXX de 20XX.

Rio de Janeiro, na data da assinatura eletrônica.



Documento assinado eletronicamente por **Rodolfo Targino de Araujo, Assistente**, em 23/03/2026, às 14:16, 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 **128115013** e o código CRC **E220E051**.

Referência: Processo nº SEI-430002/001505/2024

SEI nº 128115013

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 Informaão e Comunicaão do Estado do Rio de Janeiro
Vice Presidncia de Tecnologia

ANEXO VII

MODELO DE ORDEM DE SERVIO / FORNECIMENTO

Este anexo deve ser interpretado conforme as disposiões do Termo de Referncia do qual  parte integrante e indissocivel.

1 - IDENTIFICAO DA ORDEM DE SERVIO / FORNECIMENTO			
Nda OS/OF:	Data de Emissao:	N do Contrato:	Data do Contrato: Extrato DOERJ:

2 - IDENTIFICAO DA EMPRESA CONTRATADA			
Nome da Empresa:			
CNPJ:		Inscrio Estadual:	
Endereo:			
Cidade:		UF:	
CEP:	Telefone:		E-mail:
Preposto:			Celular: E-mail:

3 - ESPECIFICAO DOS PRODUTOS/SERVIOS E VOLUMES ESTIMADOS							
Item / Lote	ID SIGA	Descrio do Produto ou Servio	Mtrica	Valor Unitrio (R\$)	Quantidade / Volume	Valor Total do item (R\$)	Parcela R\$ (esta coluna pode ser descartada em caso de pgto a vista)

Valor Total (R\$)	
--------------------------	--

4 – INSTRUÇÕES COMPLEMENTARES

5 – CIÊNCIA	
CONTRATANTE	
Gestor do Contrato	Fiscal Requisitante do Contrato
_____ nome ID nº	_____ nome ID nº
CONTRATADA	
PREPOSTO	
_____ nome CPF:	

Rio de Janeiro, na data da assinatura eletrônica.



Documento assinado eletronicamente por **Rodolfo Targino de Araujo, Assistente**, em 23/03/2026, às 14:17, 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 **128113942** e o código CRC **5EE2034F**.

Referência: Processo nº SEI-430002/001505/2024

SEI nº 128113942

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 VIII

MODELO DE PLANILHA DE COMPOSIÇÃO DE PREÇOS

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

Processo SEI N° _____						
Ata de Registro de Preços N° ____/____						
Fornecedor:						
OBJETO:						
Lote I						
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.						
Lote II						
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.						
Lote III						
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.						
LOTE I						
ITEM	DESCRIÇÃO	MÉTRICA	FORMA DE FORNECIMENTO	QUANTIDADE ESTIMADA	Valor Unitário (R\$)	Valor Total (R\$)

1	Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	Unidade	Aquisição			
2	Serviço técnico especializado de Instalação da Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	Unidade	Sob Demanda			
3	Treinamento da Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	Aluno	Sob Demanda			
Valor total do Lote 1						
LOTE II						
ITEM	DESCRIÇÃO	MÉTRICA	FORMA DE FORNECIMENTO	QUANTIDADE ESTIMADA	Valor Unitário (R\$)	Valor Total (R\$)
4	Equipamento para a interceptação do tráfego	Unidade	Aquisição de Equipamento			
5	Licenciamento de desduplicação do tráfego.	Unidade	Subscrição de Licença por 36 meses			
6	Licenciamento avançado de description do tráfego.	Unidade	Subscrição de Licença por 36 meses			
7	Licenciamento avançado de análise de aplicações.	Unidade	Subscrição de Licença por 36 meses			

8	Licenciamento avançado de análise de análise de metadados.	Unidade	Subscrição de Licença por 36 meses			
9	Módulo de expansão do processamento.	Unidade	Aquisição de Equipamento			
10	Módulo de expansão para a captura do tráfego “inline”.	Unidade	Aquisição de Equipamento			
11	Licenciamento para o gerenciamento centralizado da solução.	Unidade	Subscrição de Licença por 36 meses			
12	Interceptor do tráfego virtualizado avançado.	Unidade	Subscrição de Licença por 36 meses			
13	Chassi para interconector passivo de interceptação do tráfego - interfaces ópticas	Unidade	Aquisição de Equipamento			
14	Interconector passivo de interceptação do tráfego – interfaces SFP	Unidade	Aquisição de Equipamento			
15	Interconector passivo de interceptação do tráfego – interfaces QSFP	Unidade	Aquisição de Equipamento			
16	Interconector passivo de interceptação do tráfego – interfaces RJ-45	Unidade	Aquisição de Equipamento			
17	Concentrador de Tráfego de Segurança.	Unidade	Aquisição de Equipamento			
18	Transceiver tipo 1 – 1 Gbps ethernet	Unidade	Aquisição de Equipamento			
19	Transceiver tipo 2 – 10 Gbps ethernet	Unidade	Aquisição de Equipamento			
20	Transceiver tipo 3 – 25 Gbps ethernet	Unidade	Aquisição de Equipamento			

21	Transceiver tipo 4 – 100 Gbps ethernet	Unidade	Aquisição de Equipamento			
22	Serviço técnico de suporte especializado para hardware, software do lote II	UST	Sob Demanda			
Valor total do Lote 2						

LOTE III						
ITEM	DESCRIÇÃO	MÉTRICA	FORMA DE FORNECIMENTO	QUANTIDADE ESTIMADA	Valor Unitário (R\$)	Valor Total (R\$)
23	Licenciamento Elastic Enterprise On-Premises.	Unidade	Subscrição de Licença por 36 meses			
24	Serviço técnico especializado para o Licenciamento Elastic Enterprise On-Premises	UST	Sob Demanda			
Valor total do Lote 1						

- Os preços deverão contemplar discriminadamente todos os custos de cada item de acordo com as condições estabelecidas no Termo de Referência.

Rio de Janeiro, na data da assinatura eletrônica.



Documento assinado eletronicamente por **Rodolfo Targino de Araujo, Assistente**, em 23/03/2026, às 14:17, 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 **128115139** e o código CRC **137ADA42**.

Referência: Processo nº SEI-430002/001505/2024

SEI nº 128115139

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 IX

MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

Identificação Contrato:	Nº da OS
Objeto:	
CONTRATANTE:	
Contratada:	

Por este instrumento, atestamos que os serviços integrantes da O.S. acima identificada, ou conforme definido no Modelo de Execução do contrato supracitado, foram recebidos nesta data e serão objetos de avaliação quanto à adequação da Solução de Tecnologia da Informação e à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato pela CONTRATANTE.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até ___ dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência do Contrato acima identificado.

De Acordo

CONTRATANTE	CONTRATADA
Membro da comissão fiscalizadora	Preposto

<p><i>Nome:</i></p> <p><i>Matrícula:</i></p>	<p><i>Nome:</i></p> <p><i>Qualificação:</i></p>
---	--

_____, _____ de _____ de 20__.

Rio de Janeiro, na data da assinatura eletrônica.



Documento assinado eletronicamente por **Rodolfo Targino de Araujo, Assistente**, em 23/03/2026, às 14:17, 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 **128115550** e o código CRC **FDA9824D**.

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 X
MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

1 – IDENTIFICAÇÃO

CONTRATO Nº		Vigência:
CONTRATADA	CNPJ	
Nº DA OS/OFB		

2 – ESPECIFICAÇÃO DOS PRODUTOS/BENS E VOLUMES DE EXECUÇÃO

SOLUÇÃO DE TIC

Objeto:

ID SIGA	Descrição do Produto ou Serviço	Métrica	Valor Unitário (R\$)	Quantidade / Volume	Valor Total (R\$)	Parcela 21/36 (R\$)
TOTAL						

3 – ATESTE DE RECEBIMENTO

Por este instrumento atestamos, que os serviços correspondentes à (link do documento) acima identificada foram prestados pela **CONTRATADA** e atendem às condições contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Termo de Referência do Contrato acima indicado.

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

5 – AUTORIZAÇÃO PARA FATURAMENTO

GESTOR DO CONTRATO

AUTORIZA-SE a **CONTRATADA** a apresentar as notas fiscais dos bens entregues relativos à supracitada (link do documento), no valor discriminado no item 2, acima.

Gestor do Contrato
Matrícula:

6 – CIÊNCIA

FISCAL TÉCNICO

Fiscal
Matrícula:

FISCAL REQUISITANTE

Fiscal
Matrícula:

PREPOSTO

Nome do Preposto da Contratada
CPF:
Nome da Contratada

Rio de Janeiro, ___ de _____ de _____

Rio de Janeiro, na data da assinatura eletrônica.



Documento assinado eletronicamente por **Rodolfo Targino de Araujo, Assistente**, em 23/03/2026, às 14:17, 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 **128116073** e o código CRC **236246FD**.

Referência: Processo nº SEI-430002/001505/2024

SEI nº 128116073

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone: