Chamada de Oportunidade de Serviços de Nuvem Pública Nº. 001/2025 – Solução de visibilidade e detecção de ameaças do tráfego de rede, aderente ao Edital de Pré-qualificação Permanente de Serviços em Nuvem Nº 001/2019 - ETICE

Junho/2025

1. OBJETO

Chamada de oportunidade para contratação de plataforma em nuvem para gerenciamento de Solução de visibilidade e detecção de ameaças do tráfego de rede e SSL Decryption Universal.

2. OBJETIVOS

Contribuindo com o aprimoramento tecnológico dos entes da Administração Pública do Estado do Ceará e reforçando sua missão de ser referência nacional como empresa de Tecnologia da Informação e Comunicação – TIC, indutora da inovação e modernização para o desenvolvimento econômico-social no fornecimento de serviços de tecnologia de alta performance em nuvem, a **ETICE** deseja selecionar, dentre as empresas pré-qualificadas, **serviços técnicos especializados para provimento de solução em nuvem**, conforme detalhamento técnico constante neste documento.

Assim, considerando as premissas estabelecidas no Edital de Pré-qualificação 001/2019, a Empresa de Tecnologia da Informação do Ceará – ETICE convoca as empresas pré-qualificadas para que apresentem propostas para **fornecimento dos serviços em nuvem, seguindo as definições técnicas deste documento convocatório**.

Todos os recursos e serviços necessários deverão ser lançados na proposta em modalidade OPEX.

Outrossim, vale destacar que os itens de serviços vencedores de cada chamada de oportunidade já serão trazidos para a composição do Marketplace da ETICE, devendo o(s) contrato(s) serem realizados por demanda; ou seja, SEM comprometimento do Orçamento da ETICE, podendo haver a contratação parcelada do objeto da presente chamada de Oportunidade; tudo consoante ao disposto nos itens 13.11, 17.1.1, 17.1.2 e 17.1.3 do Edital de Pré-qualificação, *in verbis*:

> "13.11. **Os itens de serviços vencedores de cada chamada de oportunidade serão trazidos para a composição dos serviços do *marketplace* da ETICE**, devendo seus preços finais serem mantidos como máximos por um prazo mínimo de 12 (doze) meses a contar da data da homologação do resultado da chamada de oportunidade.
>
> (...)
>
> 17.1.1. Consoante o disposto no art. 140, parágrafos 4º e 5º do Regulamento de Licitações e Contratos da ETICE, **fica desde já a ETICE autorizada a celebração de contratos por demanda**.
>
> 17.1.2. A ETICE fixará um quantitativo ou valor máximo de fornecimento ou serviço a ser utilizado no prazo de vigência do referido contrato, **SEM comprometimento do Orçamento da ETICE**.
>
> 17.1.2. Na hipótese do item anterior, a ETICE **demandará o objeto de forma PARCELADA e apenas quando necessitar, nos termos e prazos definidos no Edital e contrato**, remunerando o contratado apenas pelo que for efetivamente executado." (grifou-se)

Este documento descreve as **características funcionais, premissas técnicas e de serviços** que deverão ser consideradas pelas pré-qualificadas, para que, munidos de informações relevantes sobre as necessidades para atendimento ao escopo dos serviços, emitam propostas de acordo com as condições preestabelecidas no Edital de Pré-qualificação supracitado.

3. SOBRE O MODELO DE CONTRATAÇÃO

3.1. Esta chamada de oportunidade obedecerá ao disposto no **Edital de pré-qualificação de nuvem nº 001/2019 da ETICE e seus anexos**, nos **Termos de Pré-Qualificação** e no **Regulamento de Licitações**

e Contratos da ETICE; sendo regido, também, pela **Lei Federal 13.303/2016**, pelos **Princípios da Direito Civil** e, no que couber, pelos Princípios da Administração Pública e demais legislação correlata.

3.2. A chamada será feita em lote único visto que os itens desta chamada são intrinsecamente interconectados, o que impossibilitaria sua divisão.

3.3. **Justificativa de escolha da Plataforma da Solução de visibilidade e detecção de ameaças do tráfego de rede:**

A Solução de Visibilidade de Ameaças e do Tráfego de Rede e SSL Decryption Universal tem como foco manter a visibilidade total e contínua dos serviços de TIC, identificar acessos não autorizados, permitindo a detecção de ameaças, a filtragem de tráfego com base na visibilidade das camadas de aplicação e a identificação bidirecional, bem como a Decryption SSL Universal de forma unificada.

Justifica-se a contratação de uma Solução de visibilidade e detecção de ameaças do tráfego de rede e SSL Decryption Universal, utilizando software e ferramentas adequadas para este fim, onde as informações produzidas pelo estado tem valor inestimável para a sociedade, portanto, necessária para garantir a disponibilidade dos serviços e informações críticas fornecidos pelo estado ao público interno e externo, bem como os demais serviços associados, conforme estabelecidos neste Termo de Referência.

A infraestrutura de TIC dispõe de uma série de ativos heterogêneos que, dada a criticidade dos sistemas

hospedados, deve operar em alta disponibilidade, visibilidade e resiliência a falhas, da operação dos sistemas.

Portanto é primordial aprimorar a atuação preventiva, elevar o grau de visibilidade do tráfego da rede e a detecção de comportamentos anômalos, haja vista que a transformação digital no setor público trouxe desafios crescentes em segurança cibernética, especialmente no controle e monitoramento do tráfego de dados que circula nas redes institucionais. Com a massificação do uso de criptografia (TLS/SSL), estima-se que mais de 90% do tráfego atual é cifrado, dificultando a inspeção de ameaças ocultas em conexões seguras.

Sem mecanismos apropriados de visibilidade e decriptação universal (SSL Decryption), os órgãos públicos permanecem vulneráveis a malwares, ransomwares, spywares e outros códigos maliciosos encapsulados em fluxos criptografados, bem como a vazamentos de dados sensíveis e atividades de espionagem.

Vale destacar que os principais objetivos da Contratação, são:

- Garantir visibilidade total sobre o tráfego de rede, inclusive os fluxos cifrados em SSL/TLS;
- Detectar e mitigar ameaças avançadas (APT, Zero-day, Botnets) que se ocultam em pacotes criptografados;
- Assegurar a conformidade com normas de segurança da informação aplicáveis ao setor público, tais como o Decreto nº 10.222/2020 (Estratégia Nacional de Cibersegurança), LGPD (Lei nº 13.709/2018) e normas do GSI/PR e TCU;
- Proteger ativos críticos de TI, como datacenters, serviços de nuvem, ERPs, bancos de dados e portais públicos.

O crescimento exponencial de aplicações criptografadas impede firewalls, IPS/IDS e antivírus tradicionais de inspecionar tráfego HTTPS, sem um mecanismo universal de decriptação SSL. A ausência dessa capacidade resulta em "pontos cegos" de segurança, exploráveis por cibercriminosos.

A Ferramenta trata-se de uma solução universal para SSL/TLS, operando de forma transparente e interoperável com outros dispositivos de segurança (como SIEMs, Firewalls, IDS/IPS, Sandboxes), garantindo análise profunda (Deep Packet Inspection) sem degradação de performance ou latência crítica.

Com a decriptação SSL universal, a solução permitirá:

- Identificação de malwares disfarçados em payloads cifrados;
- Bloqueio de exfiltração de dados sigilosos por canais criptografados;
- Prevenção contra técnicas de evasão usadas por ransomwares e botnets modernos.

Atendimento integral aos Requisitos Estratégico de Governança e Compliance;

- Atende recomendações do GSI/PR, ABNT NBR ISO/IEC 27001 (Segurança da Informação) e auditorias do TCU;
- Assegura a integridade e a confidencialidade dos dados da Administração Pública;
- Reduz riscos institucionais, operacionais e reputacionais.

Destacam-se alguns Impactos diretos da não Contratação

- Falta de visibilidade sobre 90% do tráfego de rede (cifrado), favorecendo ataques indetectáveis;
- Possibilidade de violação de dados pessoais protegidos pela LGPD;
- Vulnerabilidade em auditorias e controles exigidos por órgãos fiscalizadores;
- Risco à continuidade dos serviços críticos à sociedade.

Logo, buscar minimizar os pontos de falha de segurança na visibilidade e ameaças do tráfego de rede, além das informações e dados em custódia, hospedados e processados, desenvolver estratégias que possam inibir a tentativa de busca, vazamento e sequestro de informações que possam comprometer a segurança de dados e permitir o tratamento das informações sensíveis, sujeitas às legislações e normas brasileiras, preservando níveis de sigilo, prevenindo ataques ou penalizando repasse ou acesso indevido de informações pela rede de dados são estratégias a serem adotadas com esta contratação.

Portanto, a ETICE, utilizando os princípios da padronização e continuidade, vem ao encontro do seu papel e de suas áreas de negócio, tendo em vista ser factível incluir novas soluções de TIC, permitindo maior capilaridade do portfólio de serviços da ETICE, com vasta integração no Estado do Ceará.

Considerando a quantidade de demanda dos órgãos da administração direta e indireta do Estado, bem como da própria ETICE para utilização de recursos em nuvem para provimento dos serviços de Solução de visibilidade e detecção de ameaças do tráfego de rede e SSL Decryption Universal.

Considerando que a ETICE ao fornecer uma solução de visibilidade e detecção de ameaças do tráfego de rede e SSL Decryption Universal, para vários órgãos do Estado, poderá proporcionar:

a) Redução de custos e transparência para órgãos e o estado; Controle e monitoramento com gerenciamento centralizado aos colaboradores; visando Auditoria, Governança e Conformidade em Segurança Cibernética e LGPD.

b) Inovação tecnológica. Considerando que a Solução de visibilidade e detecção de ameaças do tráfego de rede e SSL Decryption Universal, a ser implementada demonstrará ser uma solução robusta, confiável e segura;

Assim sendo, a presente chamada de oportunidade será aberta para oferta de Solução de visibilidade e detecção de ameaças do tráfego de rede e SSL Decryption Universal, em nuvem, visando expandir com novos serviços a serem adicionados no Marketplace da ETICE. A expectativa é que com uma maior disponibilidade de serviços no seu Marketplace, ampliando seu alcance de mercado, a Etice possa cumprir o disposto na Lei nº 16.727.

3.4. **Justificativa Lote Único**

3.4.1. A contratação de serviços em nuvem em lote único visa atender às demandas de infraestrutura de TI da instituição de maneira eficiente, segura e escalável, alinhando-se aos princípios da Lei 13.303/2016, conhecida como Lei das Estatais. Esta lei estabelece diretrizes para licitações e contratações realizadas por empresas públicas e sociedades de economia mista, promovendo a economicidade, eficiência, transparência e segurança jurídica nas contratações públicas.

3.4.2. A contratação de serviços em nuvem em lote único permite a negociação de pacotes de serviços com melhores condições comerciais, promovendo economia de escala. Ao centralizar a contratação em um único fornecedor, a instituição pode obter descontos significativos, reduzir custos administrativos relacionados a múltiplos contratos e otimizar o uso dos recursos disponíveis, o que está alinhado com os princípios de economicidade estabelecidos pela Lei 13.303/2016.

3.4.3. A contratação em lote único facilita a gestão e administração dos serviços em nuvem, permitindo uma visão centralizada e integrada da infraestrutura de TI. Isso reduz a complexidade operacional e melhora a governança sobre os recursos contratados, garantindo um maior controle e transparência sobre os gastos e a utilização dos serviços.

3.4.4. A contratação de serviços em nuvem em lote único permite que a instituição se beneficie de atualizações contínuas de infraestrutura e software sem custos adicionais. Além disso, disponibiliza de suporte técnico especializado e documentação abrangente, garantindo que a instituição tenha acesso a uma base de conhecimento global e suporte 24/7. Isso facilita a manutenção de um ambiente de TI robusto e resiliente, de acordo com o princípio de eficiência da Lei 13.303/2016.

3.4.5. A contratação de serviços em nuvem em lote único é justificada por proporcionar uma solução robusta, eficiente, segura e econômica para a instituição. Alinhada aos princípios da Lei 13.303/2016, essa abordagem assegura a melhor utilização dos recursos públicos, promove a inovação, garante a segurança dos dados e oferece uma gestão simplificada e centralizada. Com essas vantagens, a instituição estará bem posicionada para enfrentar os desafios da transformação digital e atender às demandas de um ambiente de negócios em constante evolução.

3.4.6. No caso em análise, a opção pelo lote único decorre da constatação de que os itens da Chamada de Oportunidade são tecnicamente interconectados e inseparáveis, pois tratam de soluções integradas de serviços em nuvem que exigem compatibilidade operacional, padronização tecnológica e integração sistêmica, de modo a assegurar eficiência, segurança da informação, interoperabilidade e gestão unificada dos serviços contratados.

3.4.7. A eventual divisão dos itens comprometeria a coerência da solução pretendida, podendo acarretar:

3.4.7.1. Riscos de incompatibilidade técnica;

3.4.7.2. Aumento de custo operacional;

3.4.7.3. Perda de controle sobre a padronização e gestão centralizada;

3.4.7.4. Redução da eficiência e da governança dos serviços contratados.

3.4.8. Cabe destacar que a jurisprudência do Tribunal de Contas da União (TCU), notadamente o Acórdão n.º 2.622/2013 – Plenário, admite a adoção de lote único desde que devidamente justificada, especialmente em situações nas quais a fragmentação do objeto comprometa a economicidade ou a viabilidade técnica da contratação.

3.4.9. Assim, a formação de lote único na presente Chamada de Oportunidade está devidamente justificada pela necessidade de garantir a integridade técnica e operacional da solução em nuvem a ser contratada, atendendo ao interesse público, à economicidade e à eficiência administrativa, conforme exigido pela Lei n.º 13.303/2016 e pelos normativos internos da ETICE.

4. CRITÉRIO DE JULGAMENTO.

4.1. **Menor Preço.**

5. ORIENTAÇÕES GERAIS

5.1. Prazos

Número do Evento	Evento	Prazo limite
1	Recebimento de propostas das empresas pré-qualificadas pela ETICE	Até 15 (quinze) dias úteis (*)
2	Pedidos de Esclarecimentos	**Até às 17h00** do 3º (terceiro) dia útil que antecede o prazo de entrega das propostas.
3	Resposta aos Pedidos de Esclarecimentos	Até 2 (dois) dias úteis, a contar do término do prazo de pedidos de esclarecimentos (**).
4	Pedidos de Impugnação	**Até às 17h00** do 3º (terceiro) dia útil que antecede o prazo de entrega das propostas.
5	Respostas à Impugnação Interposta	Até 2 (dois) dias úteis, a contar do término do prazo de pedidos de esclarecimento.
6	Avaliação, Negociação e definição da proposta vencedora pela ETICE	Até 5 (cinco) dias úteis, contados a partir do término do prazo de apresentação de propostas.
7	Interposição de Recurso	Até 5 (cinco) dias úteis, contados a partir da divulgação da proposta vencedora.
8	Apresentação de Contrarrazões ao Recurso	Até 5 (cinco) dias úteis, contados a partir do término do prazo de interposição de recurso.
9	Decisão **definitiva** da Comissão	Até 5 (cinco) dias úteis, contados a partir do término do prazo de apresentação de contrarrazões recursais, podendo variar em razão da complexidade da matéria.(***)

10	Homologação e Adjudicação	Até 5 (cinco) dias úteis, a contar da divulgação da decisão definitiva da Comissão.

(*) O prazo será contado a partir do primeiro dia útil seguinte à publicação deste documento no website da ETICE, no link https://www.etice.ce.gov.br/projeto/pre-qualificacao-permanente/.

(**) O prazo poderá ser alterado conforme disposto no item 6.4.

(***) Caso haja desistência expressa do Prazo Recursal (e consequente Contrarrazões), o Prazo para apresentação da Decisão Definitiva poderá ser reduzido, conforme o caso.

5.1.1. Os Prazos dispostos no item acima poderão variar em conformidade com o caso concreto, **podendo inclusive serem mitigados**, em razão de não apresentação de recursos ou mesmo que as empresas Pré-qualificadas declinem, formalmente, do direito Recursal (e consequentemente das contrarrazões).

5.2. Sobre o envio da Proposta Técnica.

5.2.1. **A proposta deverá ser enviada de forma eletrônica e deverá ser CRIPTOGRAFADA utilizando uma chave privada (senha).**

5.2.2. A proponente é responsável por gerar uma chave aleatória e manter completo sigilo desta chave, sem revelá-la a terceiros, nem à Etice, até que se tenha passado o período de recebimento de propostas estabelecido na tabela do item 5.1.

5.2.3. Antes ou após criptografada, **a proposta deve ser assinada digitalmente**, conforme o modelo da Medida Provisória 2.200-2/2001.

5.2.4. Com o objetivo de facilitar a submissão de propostas e considerando que vários *softwares* possibilitam a assinatura digital de um documento antes de uma encriptação e não após ela, a ETICE aceitará também propostas que tenham sido assinadas digitalmente antes de terem sido encriptadas contanto que o nome do arquivo de proposta possibilite a identificação clara do proponente.

5.2.5. A proposta criptografada e assinada deve ser enviada para o e-mail avaliacao.nuvem@etice.ce.gov.br. **O HORÁRIO DE RECEBIMENTO DAS PROPOSTAS SERÁ ATÉ ÀS 17H (DEZESSETE HORAS) DO ÚLTIMO DIA ÚTIL PARA RECEBIMENTO DAS PROPOSTAS.**

5.2.6. Uma proposta só será considerada **entregue no prazo** caso a ETICE responda com um e-mail para o proponente reconhecendo o recebimento dentro do prazo.

5.2.7. **Proposta enviada para e-mail não correto ou com erro de escrita ou que tenha sido recusada pelo servidor não será considerada entregue no prazo.**

5.2.8. A proponente deverá enviar a chave criptográfica usada para encriptar a proposta para a ETICE em até 01 (um) dia útil após encerrado o prazo de recebimento de propostas.

5.2.9. **Arquivos corrompidos ou chaves que não permitam descriptografar a proposta, tornarão a proposta nula.**

5.2.10. **Todos os recursos e serviços necessários deverão ser lançados nas propostas em modalidade OPEX e em moeda nacional (reais).**

5.2.11. Na proposta deverá constar as cotações de todos os itens de serviços especificados neste documento, expressas em reais e em valores mensais e anuais.

5.2.12. Para fins de elaboração de Proposta, as empresas participantes deverão considerar que o prazo contratual será de 12 (doze) meses, prorrogável na forma da lei.

5.2.13. A ETICE descriptografará todas as propostas válidas e ordenará tais propostas baseadas em seu valor global.

5.3. Processo de Seleção e Negociação

5.3.1. **A seleção e negociação da melhor proposta ocorrerá preferencialmente se existirem, no mínimo, 3 (três) propostas válidas para a chamada.**

5.3.2. Será considerada válida a proposta que atender aos requisitos elencados no item 5.2.

5.3.3. **Caso sejam apresentadas apenas 02 (duas) propostas válidas na chamada de oportunidade, para homologação do resultado da chamada, poderá ser realizada pesquisa de mercado para validação dos preços apresentados pelas PRÉ-QUALIFICADAS participantes da chamada, sendo vedada a contratação de empresa que não seja pré-qualificada. No caso de ser apresentada apenas 01 (uma) proposta, a Chamada será considerada fracassada.**

5.3.4. O processo de seleção e negociação respeitará as regras do edital de pré-qualificação e da presenta chamada com base na proposta mais vantajosa para a ETICE, de forma a não comprometer a economicidade.

5.3.5. **Será declarada vencedora a proposta que apresentar o menor preço.**

5.3.6. Será **Desclassificada** a Proposta vencedora que:

5.3.6.1. Contenham vícios insanáveis;

5.3.6.2. Descumpram especificações técnicas constantes desta Chamada de Oportunidade;

5.3.6.3. Apresentem preços cujo valor do item e/ou valor total seja superior ao valor estimado após a negociação para contratação, de acordo com § 1o Art. 57 da Lei nº 13.303.

5.3.6.3.1. Para declaração de sobrepreço a proposta vencedora necessariamente deve passar por negociação nos critérios do item 5.3.7, mantendo-se o segredo da estimativa.

5.3.6.3.2. A negociação deverá abordar a integralidade da proposta, não sendo restrita aos itens específicos que apresentem sobrepreço.

5.3.6.3.3. A desclassificação será mantida caso, mesmo após o processo de negociação, os preços continuem superiores ao estimado.

5.3.6.4. Apresentem preços manifestamente inexequíveis;

5.3.6.4.1. Será considerada inexequível as propostas:

5.3.6.4.1.1. Cujo valor total seja igual ou inferior a 50% abaixo do valor estimado para contratação.

5.3.6.4.1.2. Cujo valor do item da proposta seja igual ou inferior a 50% abaixo do valor estimado para aquele item.

5.3.6.4.1.3. Para declaração de inexequibilidade a proposta vencedora necessariamente deve passar pelo processo de diligência, sendo mantida a desclassificação caso não seja demonstrada a sua viabilidade técnica/operacional.

5.3.6.5. Não tenham sua exequibilidade demonstrada, quando exigido pela ETICE;

5.3.6.5.1. A Etice comprovará a exequibilidade das propostas por meio dos itens abaixo:

5.3.6.5.1.1. Nota fiscais, faturas, relatórios e medições de serviços semelhantes prestados, atestados técnicos, contratos, dentre outros.

5.3.6.6. Apresentem desconformidade com outras exigências do instrumento convocatório, salvo se for possível a acomodação a seus termos antes da adjudicação do objeto e sem que se prejudique a atribuição de tratamento isonômico entre as licitantes;

5.3.6.7. A ETICE poderá realizar diligências para aferir a exequibilidade das propostas ou exigir das licitantes que ela seja demonstrada;

5.3.6.8. A desclassificação será sempre fundamentada.

5.3.7. A negociação com a empresa declarada vencedora será feita após a sua classificação, por meio de apresentação de nova proposta com descontos percentuais que esta possa oferecer.

5.3.7.1. Será mantido o caráter sigiloso da estimativa de preço, sendo este divulgado em concomitância com a abertura do prazo recursal.

5.3.7.2. A proposta negociada deverá apresentar os mesmos valores originalmente estipulados ou com redução, não sendo aceito qualquer tipo de aumento dos valores dos itens já orçados.

5.3.7.3. A apresentação de itens com valores maiores na proposta negociada, não se tratando de erro material, ensejará a sua desclassificação.

6. ESCLARECIMENTOS

6.1. As dúvidas na interpretação do presente documento e anexos, consultas ou pedido de esclarecimentos acerca das informações técnicas porventura existentes, poderão ser feitos via e-mail de forma expressa, **clara, concisa e objetiva**, constando no corpo do texto do e-mail a identificação completa da empresa pré-qualificada participante e do representante que questiona as informações ou solicita esclarecimentos.

6.2. Os pedidos de esclarecimentos deverão ser encaminhados **até às 17h00 do 3º (terceiro) dia útil que antecede o término do prazo de apresentação das propostas**.

6.3. O endereço de e-mail para os esclarecimentos é: **avaliacao.nuvem@etice.ce.gov.br**.

6.4. A ETICE terá um prazo de até 02 (dois) dias úteis para resposta, sendo possível estender esse prazo de acordo com a complexidade dos esclarecimentos e/ou a necessidade de utilização de recursos técnicos externos à ETICE.

6.5. Caso a(s) resposta(s) dos esclarecimentos provoquem alterações das definições técnicas do projeto e estas sejam consideradas relevantes pela ETICE, será reiniciada a contagem dos prazos estabelecidos no item 5.1 deste documento, cabendo comunicação prévia e única a todas as pré-qualificadas.

6.6. **As quantidades aqui mencionadas são previsões e NÃO implicam em obrigatoriedade de contratação de quaisquer quantidades pela Administração Pública, servindo apenas como referencial para a elaboração das propostas das empresas pré-qualificadas pela ETICE.**

7. ESPECIFICAÇÃO TÉCNICA DOS SERVIÇOS

ITEM	DESCRIÇÃO	UND.	QTD.
1	Serviço de Interceptação do Tráfego – Tipo 1.	Serviço	6
2	Serviço de Interceptação do Tráfego – Tipo 2.	Serviço	4
3	Serviço de Interceptação do Tráfego - Tipo 3.	Serviço	2
4	Serviço de Descriptografia do Tráfego – Compatível com os Serviços do Tipo 1 e 2.	Serviço	10
5	Serviço de Descriptografia do Tráfego – Compatível com os Serviços do Tipo 3.	Serviço	2
6	Serviço para o Tratamento do Tráfego de Aplicações – Compatível com os Serviços do Tipo 1 e 2.	Serviço	8
7	Serviço para o Tratamento do Tráfego de Aplicações – Compatível com os Serviços do Tipo 3.	Serviço	4
8	Gerenciamento Centralizado da Solução.	Serviço	12
9	Serviço de Interceptação do Tráfego Virtualizado Essencial.	Serviço	4
10	Serviço de Interceptação do Tráfego Virtualizado Avançado.	Serviço	4
11	Serviço centralizado de Chassi para Interconector Passivo de Interceptação do Tráfego - Interfaces Ópticas	Serviço	12
12	Serviço de Interconector Passivo de Interceptação do Tráfego – Interfaces SFP	Serviço	40
13	Serviço de Interconector Passivo de Interceptação do Tráfego – Interfaces QSFP	Serviço	40
14	Serviço de Interconector Passivo de Interceptação do Tráfego – Interfaces RJ-45	Serviço	40
15	Serviço de Concentrador de Tráfego de Segurança.	Serviço	12
16	Serviço de Transceivers Tipo 1 – 1 Gbps Ethernet	Serviço	40
17	Serviço de Transceivers Tipo 2 – 10 Gbps Ethernet	Serviço	40
18	Serviço de Transceivers Tipo 3 – 25 Gbps Ethernet	Serviço	40
19	Serviço de Transceivers Tipo 4 – 40 Gbps Ethernet	Serviço	40
20	Serviço de Transceivers Tipo 5 – 100 Gbps Ethernet	Serviço	40
21	Serviços de Operação Assistida e ajuste fino para as Soluções de NPB	UST	40.000

7.1. **ESPECIFICAÇÃO DETALHADA**

7.1.1. A especificação detalhada dos itens 1 a 21 estão descritas no ANEXO A – CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS DE SOLUÇÃO DE VISIBILIDADE E DETECÇÃO DE AMEAÇAS DO TRÁFEGO DE REDE E SSL DECRYPTION UNIVERSAL COM GERÊNCIA EM NUVEM.

8. DA VIGÊNCIA DO CONTRATO

8.1. Os prazos de vigência e de execução contratual serão de 12 (doze) meses, podendo ser prorrogado a critério da Contratante, com concordância da contratada, por períodos iguais ou inferiores, conforme art. 71 da Lei Federal 13.303/2016 e do art. 148 do Regulamento de Licitações e Contratos da ETICE.

8.2. Referido contrato poderá ser alterado nos casos previstos no art. 81 da Lei Federal n°13.303/2016 e no art. 149 do Regulamento de Licitações e Contratos da ETICE.

9. DO MODELO DE PROPOSTA

9.1. O modelo de proposta encontra-se no ANEXO F.

10. ACORDO DE NÍVEIS DE SERVIÇOS – SLA

10.1. A gestão e fiscalização do contrato dar-se-ão mediante o estabelecimento e acompanhamento de indicadores de desempenho, disponibilidade e qualidade, que comporão o Acordo de Nível de Serviço (SLA) entre a Contratante e Contratada.

10.2. O Acordo de Nível de Serviço está especificado no ANEXO E da presente Chamada de Oportunidade.

11. CONFIDENCIALIDADE DOS TRABALHOS

11.1. A Contratada, seu preposto e qualquer profissional dela, envolvidos na realização dos trabalhos, obrigam-se a tratar todas as informações obtidas junto à ETICE e seu cliente final como informação sigilosa ou confidencial, devendo neste sentido mantê-las sob estrito sigilo, comprometendo-se ainda em não comunicar, divulgar ou revelar as informações confidenciais a terceiros, mesmo após a finalização dos trabalhos a confidencialidade das informações permanece.

11.2. Para tal, serão consideradas como informações confidenciais todas e quaisquer informações ou dados, independentemente de estarem expressamente classificados como confidenciais, fornecidas verbalmente ou por escrito, ou de qualquer outra forma, corpórea ou não, cuja divulgação possa provocar prejuízos de qualquer natureza, abrangendo, mas não se limitando a, pormenores, estratégias de negócios, pesquisas, dados financeiros e estatísticos, informações sobre negociações em andamento, informações sobre

softwares, informações cadastrais, documentos que venha a ter conhecimento ou acesso, ou que venha a receber da contratante, sejam de caráter técnico ou não.

11.3. Tais informações confidenciais deverão ser usadas exclusivamente para a condução dos trabalhos objeto da relação de serviços entre a ETICE, cliente final e a contratante, não podendo, sob nenhuma forma ou pretexto, serem divulgadas, reveladas, reproduzidas, utilizadas ou ser dado conhecimento a terceiros estranhos a esta contratação, exceto quando o dever de divulgar tais informações seja estritamente por força de exigência legal, devendo a parte obrigada a fornecer tais informações, avisar imediatamente a outra parte sobre tal exigência legal para, se for o caso, tomar as providências que achar necessárias.

11.4. A Contratada deverá apresentar "Termo de Responsabilidade e Sigilo", contendo a declaração de manutenção de sigilo e ciência das normas de segurança da ETICE, assinado por cada empregado seu que estiver diretamente envolvido na contratação, quando o serviço exigir.

11.5. A contratada deverá entregar à ETICE, no momento da rescisão do contrato, todo o material físico ou digital de propriedade da contratante e destruir qualquer cópia em posse da contratada.

12. DA FRAUDE E DA CORRUPÇÃO

12.1. As Pré-Qualificadas devem observar e a contratada deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual.

12.2. Para os propósitos deste item, definem-se as seguintes práticas:

12.2.1. **“prática corrupta”:** oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

12.2.2. **“prática fraudulenta”:** a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

12.2.3. **“prática conluiada”:** esquematizar ou estabelecer um acordo entre duas ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não- competitivos;

12.2.4. **“prática coercitiva”:** causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas, ou sua propriedade, visando a influenciar sua participação em um processo licitatório ou afetar a execução do contrato;

12.2.5. **“prática obstrutiva”:**

12.2.5.1. destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista neste subitem;

12.2.5.2. atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

12.3. Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, conluiadas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.

12.4. Considerando os propósitos dos itens acima, a pré qualificada vencedora como condição para a contratação, deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.

12.5. A contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas na Lei, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

13. DA SUBCONTRATAÇÃO

13.1. Será admitida a subcontratação no limite de até 30% (trinta por cento) do objeto, conforme disposto no art. 78 da Lei nº 13.303/2016 e nos arts. 143 a 147 do Regulamento de Licitações e Contratos da ETICE, desde que não constitua o escopo principal da contratação, e, se previamente aprovada pela ETICE.

13.2. A subcontratação de que trata esta cláusula, **não exclui a responsabilidade da contratada perante a ETICE quanto à qualidade do objeto contratado, não constituindo, portanto, qualquer vínculo contratual ou legal da ETICE com a subcontratada.**

13.3. A empresa subcontratada deverá atender, em relação ao objeto da subcontratação, as exigências de qualificação técnica impostas a pré qualificada vencedora.

13.4. É **vedada** a subcontratação de empresa ou consórcio que tenha participado:

13.4.1. Do procedimento licitatório do qual se originou a contratação.

13.4.2. Direta ou indiretamente, da elaboração de projeto básico ou executivo.

14. DAS OBRIGAÇÕES DA CONTRATADA

14.1. Prestar os serviços de forma alinhada aos termos especificados no presente documento, no Contrato e na Proposta Comercial, responsabilizando-se integralmente pela exploração e execução do serviço perante a Contratante.

14.2. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

14.3. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitados ao estabelecido no §1º, do art. 81, da Lei Federal nº 13.303/2016, tomando-se por base o valor contratual.

14.4. Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.

14.5. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado para execução contratual, não transferindo a responsabilidade à ETICE para nenhum fim de direito.

14.6. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela ETICE, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

14.7. Refazer o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações deste termo, contado da sua notificação.

14.8. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta, observando o prazo mínimo exigido pela Administração.

14.9. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização da ETICE.

14.10. Responsabilizar-se por todos os direitos e obrigações contratados, mesmo que transfira para autorizadas técnicas parte dos serviços contratados.

14.11. Comunicar ao gestor do contrato, por escrito, qualquer fato relacionado ao uso indevido do equipamento, para providências por parte da CONTRATANTE.

14.12. Comunicar antecipadamente a realização de intervenções nos ambientes técnicos da Contratante entre datacenters, no caso de qualquer possibilidade de impacto na prestação dos serviços.

14.13. Assinar Termo de Confidencialidade e Sigilo, resguardando que os recursos, dados e informações de propriedade da Contratante, e quaisquer outros, repassados por força do objeto do contrato, constituem informação privilegiada e possuem caráter de confidencialidade e sigilo.

14.14. Manter, sob as penas da Lei, o mais completo e absoluto sigilo sobre quaisquer dados, informações, documentos, especificações técnicas e comerciais dos bens da Contratante, de que venha a tomar conhecimento ou ter acesso, ou que venham a ser confiados, sejam relacionados ou não com a prestação de serviços objeto do contrato.

14.15. Respeitar a legislação relativa à disposição final ambientalmente adequada dos resíduos gerados, mitigação dos danos ambientais por meio de medidas condicionantes e de compensação ambiental e outros, conforme § 1º do art. 32 da Lei 13.303/2016.

15. DAS OBRIGAÇÕES DA CONTRATANTE

15.1. Solicitar a execução do objeto à contratada através da emissão de Ordem de Serviço/Fornecimento.

15.2. Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal no 13.303/2016 e, subsidiariamente, a Lei Federal n° 8.666/1993.

15.3. Fiscalizar a execução do objeto contratual através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

15.4. Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.

15.5. Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste contrato.

15.6. Aplicar as penalidades previstas em lei e neste instrumento.

15.7. Não obstante a Contratada seja a única e exclusiva responsável pela execução dos serviços especificados, a Contratante reserva-se o direito de exercer a mais ampla, irrestrita, permanente e completa fiscalização, diretamente ou por outros prepostos designados, podendo, em decorrência, solicitar providências da Contratada, que atenderá ou justificará de imediato.

15.8. Permitir o acesso dos empregados da Contratada, quando necessário, para execução dos serviços e prestar as informações e os esclarecimentos que venham a ser solicitados pela Contratada.

16. DAS DISPOSIÇÕES GERAIS

16.1. **Esta chamada de oportunidade não implica necessariamente em contratação**, nos moldes já dispostos Edital de Pré-Qualificação 001/2019, podendo a autoridade competente revogá-la por razões de interesse público, anulá-la por ilegalidade de ofício ou por provocação de terceiros, mediante decisão devidamente fundamentada, sem quaisquer reclamações ou direitos à indenização ou reembolso.

16.2. É facultada à Comissão de Avaliação ou à autoridade competente, em qualquer fase da licitação, a **promoção de diligência** destinada a esclarecer ou a complementar a instrução do processo licitatório, vedada a inclusão posterior de documentos que deveriam constar originariamente na proposta e na documentação.

16.3. Toda a documentação fará parte dos autos e **não será devolvida à pré-qualificada**, ainda que se trate de originais.

16.4. Na contagem dos prazos estabelecidos nesta Chamada de Oportunidade, excluir-se-ão os dias de início e incluir-se-ão os dias de vencimento. Os prazos estabelecidos neste edital para a fase externa se iniciam e se vencem somente em dias úteis de expediente da ETICE.

16.5. Os representantes legais das Pré-Qualificadas são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

16.6. O desatendimento de exigências meramente formais, não essenciais, não implicará no afastamento da Pré-Qualificada, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

16.7. **A Comissão de Avaliação poderá sanar erros formais que NÃO acarretem prejuízos para o objeto da Chamada de Oportunidade**, a Administração e as Pré-Qualificadas, dentre estes, os decorrentes de operações aritméticas.

16.8. Desde já fica estabelecido que caso a Pré-Qualificada **NÃO APRESENTE PROPOSTA** para a presente Chamada de Oportunidade, já está **renunciando**, assim, **expressamente ao direito de recurso e respectiva contrarrazões, concordando com o curso desta Chamada de Oportunidade de Serviços de Nuvem Pública**, aderente ao Edital de Pré-Qualificação Permanente de Serviços em Nuvem NO 001/ 2019 - ETICE.

16.9. Os casos omissos serão resolvidos pela Comissão de Avaliação, nos termos da legislação pertinente.

16.10. As normas que disciplinam esta Chamada de Oportunidade serão sempre interpretadas em favor da ampliação da disputa.

16.11. Os documentos referentes aos orçamentos, bem como o valor estimado da contratação, possuem caráter sigiloso e serão disponibilizados em concomitância com a abertura do prazo recursal, em conformidade com o Regulamento de Licitações e Contratos da ETICE.

16.12. O **foro** designado para julgamento de quaisquer questões judiciais resultantes deste edital será o da **Comarca de Fortaleza**, Capital do Estado do Ceará.

Fortaleza,

De Acordo:	**Aprovo:**
Márcio Adriano Castro Lima *Diretor* *Diretoria de Tecnologia e Inovação (DITEC)*	**Francisco Antônio Martins Barbosa** *Presidente da Etice*

ROL DE ANEXOS:

ANEXO A – CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS DE SERVIÇOS DE SOLUÇÃO DE VISIBILIDADE E DETECÇÃO DE AMEAÇAS DO TRÁFEGO DE REDE E SSL DECRYPTION UNIVERSAL COM GERÊNCIA EM NUVEM.

ANEXO B - CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS DE SOLUÇÃO DE VISIBILIDADE E DETECÇÃO DE AMEAÇAS DO TRÁFEGO DE REDE E SSL DECRYPTION, INSTALAÇÃO CONFIGURAÇÃO E TESTES (ITENS 1 A 21).

ANEXO C - MANUTENÇÃO E SUPORTE TÉCNICO

ANEXO D - CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS DE GERENCIAMENTO, ORQUESTRAÇÃO DA NUVEM, SUSTENTAÇÃO EMERGENCIAL, ADMINISTRAÇÃO DOS PROJETOS

ANEXO E - CATÁLOGO DE SERVIÇOS

ANEXO F - LISTA DE PERFIS TÉCNICOS

ANEXO G - DO ACORDO DE NÍVEIS DE SERVIÇOS – SLA

ANEXO H - MODELO DE PROPOSTA

ANEXO A - CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS

1. ESPECIFICAÇÃO DETALHADA

SERVIÇO DE SOLUÇÃO DE VISIBILIDADE E DETECÇÃO DE AMEAÇAS DO TRÁFEGO DE REDE E SSL DECRYPTION UNIVERSAL COM GERÊNCIA EM NUVEM

A solução deve ser fornecida incluindo disponibilização de equipamento e software, instalação, configuração e testes conforme características e especificações descritas nos ANEXOS A e B.

SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO C.

1.1. CARACTERÍSTICAS GERAIS

1.1.1. 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.

1.1.2. A Solução de visibilidade ofertada deverá possuir funcionalidades e disponibilização de equipamentos 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.

1.1.3. Todos os serviços de Interceptação do Tráfego dos tipos 1, 2 e 3 ofertados, deverão atender as exigências aqui descritas integralmente.

1.1.4. Não será permitida a composição da solução ofertada entre diversos fabricantes, bem como não serão aceitas solução de software livre; ou seja, os serviços de Interceptação do Tráfego dos tipos 1, 2 e 3 ofertados, deverão ser de um único fabricante.

1.1.4.1. Quando a oferta for composta por mais de 1 (um) fabricante, para os demais itens, por exemplo um serviço de análise avançada, (Tipos 1,2 e 3) por exemplo, pertencer a um fabricante distinto, caberá a CONTRATADA prover todos os serviços de integração

da solução, de modo que o resultado da implantação deverá corresponder a disponibilidade e execução técnica de todos os requisitos aqui previstos.

1.1.5. Toda a oferta de softwares, mesmo quando condicionados a disponibilização de módulos físicos/equipamentos específicos, deverá ser fornecida na modalidade de subscrição.

1.1.5.1. 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.

1.1.6. Deverá possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas de “rede”, “rede inline”, “ferramenta” e portas de “ferramenta inline”.

1.1.6.1. Entende-se por portas de “rede”, todas as portas que serão responsáveis por receber a cópia do tráfego através dos TAPs/SPANs.

1.1.6.2. 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.

1.1.6.3. 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.

1.1.6.4. 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.

1.1.7. A Solução de visibilidade ofertada deve estar em conformidade com o padrão RoHS.

1.1.8. Deverá possuir módulos de ventilação hot swappable;

1.1.9. Possuir ventilação "front-to-back", ou seja, a saída de ar quente deve acontecer pela traseira do equipamento.

1.1.10. Deverá possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable.

1.1.10.1. Deverá vir acompanhada de seus respectivos cabos de energização padrão C13- C14.

1.1.11. A Solução deverá contemplar o máximo de fontes de alimentação suportadas por tipo de equipamento. As fontes deverão ser do tipo AC redundantes, internas ao chassi e do tipo hot- swappable.

1.1.12. Deverá suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento

1.2. **CARACTERÍSTICAS DE GERENCIAMENTO DA SOLUÇÃO**

1.2.1. Deverá possuir, no mínimo, 1 (uma) interface exclusiva ao gerenciamento remoto do equipamento disponibilizado.

1.2.1.1. As interfaces deverão vir acompanhadas de seus respectivos cabos UTP de, no mínimo, 1,0m (um metro) e com conectores RJ-45.

1.2.2. Deverá permitir configuração customizada baseadas nos perfis de acesso (RBAC - Role Base Access Control).

1.2.3. Deverá implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.

1.2.4. Deverá possuir suporte a MIB II.

1.2.5. Deverá implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.

1.2.6. Deverá suportar SNMP trap sobre IPv6.

1.2.7. Deverá permitir a atualização remota do sistema operacional e arquivos de configuração utilizados na Solução de visibilidade oferta da via interface de gerenciamento.

1.2.8. Deverá permitir a gravação de log externo (syslog).

1.2.9. 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

1.2.10. Deverá possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como estatísticas de utilização e log de eventos.

1.2.11. Deve suportar configuração total da solução através de console local RS-232 ou RJ-45.

1.2.12. Deve possuir gerenciamento através de interface Web (HTTPS) ou CLI.

1.2.13. Deverá implementar o protocolo NTP (Network Time Protocol).

1.2.14. Deverá implementar mecanismo de autenticação para acesso local ou remoto a Solução de visibilidade ofertada, baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+, RADIUS e LDAP.

1.2.15. Deve suportar IPv6 para TACACS+.

1.2.16. Deverá implementar o protocolo SSHv2 para acesso à interface de linha de comando.

1.2.17. Deverá proteger a interface de comando da Solução de visibilidade ofertada, através de senha.

1.2.18. 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 equipamento disponibilizados físicos e virtuais, nuvem e containers;

1.3. **CARACTERÍSTICAS DE SEGURANÇA**

1.3.1. 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:

1.3.1.1. Uma para uma (1 : 1);

1.3.1.2. Uma para várias (1 : N) - Com suporte ao balanceamento;

1.3.1.3. Várias para uma (N : 1);

1.3.1.4. Várias para várias (N : N) - Com suporte ao balanceamento;

1.3.2. Deverá permitir criar filtros (regras) baseados em, no mínimo, os seguintes campos:

1.3.2.1. Endereços MAC de origem e destino;

1.3.2.2. Endereço IPv4 de origem/destino;

1.3.2.3. Portas TCP e UDP de origem e destino;

1.3.2.4. VLAN ID;

1.3.2.5. Ethertype;

1.3.2.6. IPFrag;

1.3.2.7. TTL;

1.3.2.8. TOS;

1.3.2.9. Protocol;

1.3.2.10. TCP Control Mask/Bits;

1.3.2.11. DSCP;

1.3.2.12. Versão do Protocolo IPv4 e IPv6;

1.3.2.13. Endereço IPv6 de origem/destino;

1.3.3. 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.

1.3.4. Deve suportar overlapping de filtros (regras), ou seja, utilização conjunta de filtros de entrada (ingress) e filtros de saída (egress).

1.3.5. A solução deverá implementar funcionalidade Mesh/Cluster.

1.3.5.1. O Mesh/Cluster deverá permitir a configuração e gerenciamento de 2 (dois) ou mais equipamentos como um única Solução de visibilidade ofertada lógico. Não serão aceitas soluções em cascateamento (empilhamento) para o atendimento desta funcionalidade.

1.3.5.2. A solução deverá suportar, no mínimo, 30 (trinta) equipamentos em modo Mesh/Cluster.

1.3.6. O Mesh/Cluster deverá permitir a configuração de todos os Agregadores a partir de uma única interface WEB (HTTPS) e CLI.

1.3.7. A funcionalidade de Mesh/Cluster deverá suportar a criação de 1 (um) ou mais filtros (regras) que se utilizem de “portas de rede” em um equipamento físico e direcionem este tráfego para “portas de ferramenta” localizadas em outro equipamento físico, independentemente da quantidade de ativos de rede e/ou de processamento entre estes equipamentos. Não serão aceitas soluções em cascateamento/empilhadas para o atendimento deste item.

1.3.8. 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.

1.3.9. Deve suportar o conceito de FABRIC que permite a criação de filtros que se estendem por múltiplos equipamentos ou mesh/clusters de equipamentos.

1.3.10. 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.

1.4. **REDUNDÂNCIA E ALTA DISPONIBILIDADE**

1.4.1. Todos os equipamentos disponibilizados na solução devem operar em alta disponibilidade e suportar instalação em redes diferentes.

1.4.1.1. 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.

1.4.2. Caso o equipamento principal, disponibilizado na Solução de visibilidade ofertada, sofra uma interrupção, os novos tráfegos não deverão ser bloqueados, isto é, deve permitir o bypass sem prejudicar o acesso do cliente.

1.5. **FUNCIONALIDADES PARA O TRÁFEGO INTERCEPTADO EM LINHA**

1.5.1. A Solução de visibilidade ofertada deve suportar instalação sem necessidade de reconfiguração de roteadores e switches, quando utilizado no modo de operação inline (em linha).

1.5.2. A Solução de visibilidade ofertada deve suportar, de forma simultânea e em interfaces distintas, os modos:

1.5.2.1. TAP/SPAN (Cópia de Tráfego);

1.5.2.2. Inline (Tráfego de Produção);

1.5.3. 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.

1.5.4. 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.

1.5.5. A solução deverá permitir a configuração conjunta das funcionalidades serial e paralelo, permitindo criar uma sequência serial de ferramentas que estão em paralelo.

1.5.6. 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.

1.5.6.1. 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.

1.5.7. 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.

1.5.8. 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.

1.5.9. 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.

1.6. **TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO**

1.6.1. Deve suportar funcionalidade túnel (Tunnel), que permite encapsulamento e desencapsulamento de tráfego entre 2 (dois) equipamentos através de redes L3 (roteadas).

1.6.2. 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.

1.6.3. Deve suportar o balanceamento de carga dos pacotes de encapsulamento IPv6 L2GRE.

1.6.4. A solução deverá suportar balanceamento entre diferentes túneis, permitindo utilizar duas ou mais ferramentas da mesma solução como destino para todo o tráfego encapsulado.

2. ITEM 01 – SERVIÇO DE INTERCEPTAÇÃO DO TRÁFEGO – TIPO 1.

2.1. **CARACTERÍSTICAS TÉCNICAS**

2.1.1. A Solução de visibilidade ofertada deve ser baseado em equipamento disponibilizado em módulo suportando montagem em rack de 19”, com altura de no máximo 1-RU (uma unidade de altura), com fornecimento dos respectivos conjuntos de fixação.

2.1.2. O equipamento disponibilizado A Solução deverá contemplar suas devidas licenças, de funcionalidades ou de sistema operacional, que permitem a execução das técnicas previstas nesta especificação técnica.

2.1.3. 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.

2.2. **CARACTERÍSTICAS DE DESEMPENHO**

2.2.1. A Solução de visibilidade ofertada deverá possuir a capacidade de processamento de, no mínimo, 600 Gbps (seiscentos gigabits por segundo) de tráfego agregado para aplicação dos filtros (regras) descritos nesta especificação.

2.2.1.1. Esta capacidade poderá ser alcançada através da adição de módulos ou licenças.

2.2.2. A Solução de visibilidade ofertada deverá suportar, no mínimo, 16.000 (dezesseis mil) filtros (regras) de entrada e saída por modulo.

2.2.3. A Solução de visibilidade ofertada deverá possuir capacidade de processamento agregado de, no mínimo, 24 (vinte e quatro) Gbps de throughput, específico para o processamento de Deduplicação.

2.3. **CARACTERÍSTICAS DE SEGURANÇA DA INFORMAÇÃO**

2.3.1. A Solução de visibilidade ofertada ou módulo deverá atender a todas as características previstas no anexo “A” deste Edital.

2.3.2. Deve suportar a funcionalidade Packet De-Duplication (De-duplicação de Pacotes), enviando somente uma única cópia do pacote para as Ferramentas.

2.3.3. A funcionalidade de Packet De-Duplication deve suportar de-duplicação de pacotes IPv4, IPv6 e pacotes sem IP, devendo levar em consideração o Payload e os cabeçalhos ethernet.

2.3.4. 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.

2.3.5. 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:

2.3.5.1. IPv4 ToS;

2.3.5.2. IPv6 TC;

2.3.5.3. Número da Sequência TCP;

2.3.5.4. VLAN ID.

2.4. **INTERFACES DE COMUNICAÇÃO**

2.4.1. A Solução deverá contemplar, no mínimo, 12 (doze) interfaces padrão Ethernet 10/1Gbps SFP.

2.4.1.1. A Solução de visibilidade ofertada deverá disponibilizar 4 (quatro) Transceivers 10Gbps SFP+ de curto alcance, com suas respectivas fibras OM4 UPC de 5,0m.

2.4.2. A Solução de visibilidade ofertada deverá disponibilizar 4 (quatro) interfaces padrão Ethernet 100/1000Mbps RJ-45.

2.4.2.1. A Solução de visibilidade ofertada deverá disponibilizar 2 (dois) cabos UTP de, no mínimo, 5,0m (cinto metros) e com conectores RJ-45.

3. ITEM 02 – SERVIÇO DE INTERCEPTAÇÃO DO TRÁFEGO – TIPO 2.

3.1. **CARACTERÍSTICAS TÉCNICAS**

3.1.1. A Solução de visibilidade ofertada deve ser baseado em equipamento disponibilizado em módulo suportando montagem em rack de 19”, com altura de no máximo 1-RU (uma unidade de altura), com fornecimento dos respectivos conjuntos de fixação.

3.1.2. A Solução deverá contemplar suas devidas licenças, de funcionalidades ou de sistema operacional, que permitem a execução das técnicas previstas nesta especificação técnica.

3.1.3. 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.

3.2. **CARACTERÍSTICAS DE DESEMPENHO**

3.2.1. A Solução de visibilidade ofertada deverá possuir a capacidade de processamento de, no mínimo, 1800 Gbps (mil e oitocentos gigabits por segundo) de tráfego agregado para aplicação dos filtros (regras) descritos nesta especificação.

3.2.1.1. Esta capacidade poderá ser alcançada através da adição de módulos ou licenças.

3.2.2. A Solução de visibilidade ofertada deverá suportar, no mínimo, 36.000 (trinta e seis mil) filtros (regras) de entrada e saída por modulo.

3.2.3. A Solução de visibilidade ofertada deverá possuir capacidade de processamento agregado de, no mínimo, 116 (cento e dezesseis) Gbps de throughput, específico para o processamento de Deduplicação.

3.3. **CARACTERÍSTICAS DE SEGURANÇA DA INFORMAÇÃO**

3.3.1. A Solução de visibilidade ofertada ou módulo deverá atender a todas as características previstas no tópico “CARACTERÍSTICAS GERAIS SOBRE TODOS OS EQUIPAMENTOS”.

3.3.2. Deve implementar a funcionalidade Packet De-Duplication (De-duplicação de Pacotes), enviando somente uma única cópia do pacote para as Ferramentas.

3.3.3. 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.

3.3.4. 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.

3.3.5. 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:

3.3.5.1. IPv4 ToS;

3.3.5.2. IPv6 TC;

3.3.5.3. Número da Sequência TCP;

3.3.5.4. VLAN ID.

3.4. **INTERFACES DE COMUNICAÇÃO**

3.4.1. A Solução deverá contemplar, no mínimo, 8 (oito) interfaces padrão Ethernet 25/10/1Gbps SFP.

3.4.1.1. A Solução de visibilidade ofertada deverá disponibilizar 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.

3.4.2. A Solução de visibilidade ofertada deverá disponibilizar 4 (quatro) interfaces padrão Ethernet 100/40Gbps QSFP28.

4. ITEM 03 – SERVIÇO DE INTERCEPTAÇÃO DO TRÁFEGO – TIPO 3.

4.1. CARACTERÍSTICAS TÉCNICAS

4.1.1. A Solução de visibilidade ofertada deve ser baseado em equipamento disponibilizado em módulo suportando montagem em rack de 19”, com altura de no máximo 3-RU (três unidades de altura), com fornecimento dos respectivos conjuntos de fixação.

4.1.2. A Solução deverá contemplar suas devidas licenças, de funcionalidades ou de sistema operacional, que permitem a execução das técnicas previstas nesta especificação técnica.

4.1.3. 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.

4.2. CARACTERÍSTICAS DE DESEMPENHO

4.2.1. A Solução de visibilidade ofertada deverá possuir a capacidade de processamento de, no mínimo, 6400 Gbps (seis mil e quatrocentos gigabits por segundo) de tráfego agregado para aplicação dos filtros (regras) descritos nesta especificação.

4.2.1.1. Esta capacidade poderá ser alcançada através da adição de módulos ou licenças.

4.2.2. A Solução de visibilidade ofertada deverá suportar, no mínimo, 6.000 (seis mil) filtros (regras) de entrada e saída por modulo.

4.2.3. Deverá implementar capacidade de processamento agregado de, no mínimo, 232 (duzentos e trinta e dois) Gbps de throughput, específico para o processamento de Deduplicação.

4.3. **CARACTERÍSTICAS DE SEGURANÇA DA INFORMAÇÃO**

4.3.1. A Solução de visibilidade ofertada ou módulo deverá atender a todas as características previstas no anexo “A” deste Edital.

4.3.2. Deve suportar a funcionalidade Packet De-Duplication (De-duplicação de Pacotes), enviando somente uma única cópia do pacote para as Ferramentas.

4.3.3. A funcionalidade de Packet De-Duplication deve suportar de-duplicação de pacotes IPv4, IPv6 e pacotes sem IP, devendo levar em consideração o Payload e os cabeçalhos ethernet.

4.3.4. 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.

4.3.5. 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:

4.3.5.1. IPv4 ToS;

4.3.5.2. IPv6 TC;

4.3.5.3. Número da Sequência TCP;

4.3.5.4. VLAN ID.

4.4. **INTERFACES DE COMUNICAÇÃO**

4.4.1. A Solução deverá contemplar, no mínimo, 8 (oito) interfaces padrão Ethernet 100/40Gbps QSFP28.

4.4.1.1. A Solução de visibilidade ofertada deverá disponibilizar 2 (dois) transceivers 100Gbps QSFP28 de curto alcance.

4.4.1.2. A Solução de visibilidade ofertada deverá permitir a subdivisão de suas interfaces através de cabos breakout, suportando, no mínimo, 24 (vinte e quatro) interfaces.

5. ITEM 04 – SERVIÇO DE DESCRIPTOGRAFIA DO TRÁFEGO – COMPATÍVEL COM OS SERVIÇOS DO TIPO 1 E 2.

5.1. CARACTERÍSTICAS TÉCNICAS

5.1.1. A Solução ofertada deverá corresponder a 1 (um) módulo o qual possibilita a expansão da quantidade de interfaces de interceptação do tráfego de rede dos equipamentos Tipo 1 ou Tipo 2.

5.1.2. O licenciamento complementar 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.

5.2. CARACTERÍSTICAS DE DESEMPENHO

5.2.1. Deverá implementar um throughput exclusivo de tráfego criptografado de, no mínimo, 4,6 (quatro vírgula seis) Gbps, respeitando as demais condições técnicas previstas para segurança da informação.

5.3. CARACTERÍSTICAS DE SEGURANÇA DA INFORMAÇÃO

5.3.1. Deve implementar a funcionalidade SSL Decryption através de função Man-In-The-Middle e também somente cópia do tráfego.

5.3.2. A descriptografia deve ser baseada no handshake SSL/TLS e não através de portas pré- definidas.

5.3.3. A Solução de visibilidade ofertada deve permitir importação de no mínimo 1.000 (hum mil) certificados em formato PKCS #12 ou PEM.

5.3.4. 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;

5.3.5. Implementar no mínimo 100 mil conexões SSL simultâneas utilizando criptografia de 2048 bits;

5.3.6. A Solução de visibilidade ofertada deve implementar, no mínimo, os seguintes algoritmos de troca de chaves com autenticação:

5.3.6.1. RSA;

5.3.6.2. DHE;

5.3.6.3. DHE_RSA;

5.3.6.4. ECDHE com PFS (Perfect Forward Secrecy)

5.3.6.5. ECDHE_RSA;

5.3.6.6. ECDHE_ECDSA;

5.3.7. A Solução de visibilidade ofertada deve implementar, no mínimo, os seguintes métodos de autenticação de mensagens:

5.3.7.1. SHA;

5.3.7.2. SHA256;

5.3.7.3. SHA384;

5.3.7.4. POLY1305;

5.3.8. Deverá implementar Host Categorization, permitindo selecionar tráfegos que não serão descriptografados, como dados financeiros por exemplo.

5.3.9. A funcionalidade SSL Decryption se suportar, no mínimo, os seguintes protocolos:

5.3.9.1. SSL 3;

5.3.9.2. TLS 1.0;

5.3.9.3. TLS 1.1;

5.3.9.4. TLS 1.2;

5.3.9.5. TLS 1.3.

5.3.10. Deve suportar chaves de 1024 bits, 2048 bits e 4096 bits.

5.3.11. A Solução de visibilidade ofertada deve suportar, no mínimo, as seguintes cifras de criptografia:

5.3.11.1. AES_128_CBC;

5.3.11.2. AES_256_CBC;

5.3.11.3. AES_256_GCM;

5.3.11.4. CHACAH20;

5.3.11.5. Camellia128;

5.3.11.6. Camellia256;

5.3.11.7. DES_CBC;

5.3.11.8. 3DES_EDE_CBC;

5.3.11.9. SEED;

5.3.11.10. IDEA;

5.3.11.11. Chacah20-Poly1305.

5.4. **ALTA DISPONIBILIDADE**

5.4.1. Quando implementado em alta disponibilidade, em caso de falha de um dos equipamentos disponibilizados, a inspeção SSL deverá ser realizada pelo outro equipamento.

5.4.2. Deve fazer ou permitir a opção de bypass do tráfego caso falhe o TLS handshake.

5.4.3. 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.

5.4.4. 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;

5.4.5. 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.

5.5. **INTERFACES DE COMUNICAÇÃO**

5.5.1. Deverá fornecer, no mínimo, 6 (seis) pares de interfaces Ethernet 10Gb para a interconexão de fibras padrão LC-LC, do tipo “by-pass”.

6. ITEM 05 – SERVIÇO DE DESCRIPTOGRAFIA DO TRÁFEGO – COMPATÍVEL COM OS SERVIÇOS DO TIPO 3.

6.1. **CARACTERÍSTICAS TÉCNICAS**

6.1.1. A Solução ofertada deverá corresponder a 1 (um) módulo o qual possibilita a expansão da quantidade de interfaces de interceptação do tráfego de rede da Solução de visibilidade ofertada Tipo 3.

6.1.2. O licenciamento complementar 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.

6.2. **CARACTERÍSTICAS DE DESEMPENHO**

6.2.1. Deverá implementar um throughput exclusivo de tráfego criptografado de, no mínimo, 14,4 (catorze vírgula quatro) Gbps, respeitando as demais condições técnicas previstas para segurança da informação.

6.3. **CARACTERÍSTICAS DE SEGURANÇA DA INFORMAÇÃO**

6.3.1. Deve implementar a funcionalidade SSL Decryption através de função Man-In-The-Middle e também somente cópia do tráfego.

6.3.2. A descriptografia deve ser baseada no handshake SSL/TLS e não através de portas pré- definidas.

6.3.3. A Solução de visibilidade ofertada deve permitir importação de no mínimo 1.000 (hum mil) certificados em formato PKCS #12 ou PEM.

6.3.4. Implementar no mínimo de 26 mil novas conexões SSL por segundo, utilizando cifra 'TLS_RSA_WITH_AES_128_CBC_SHA256' e criptografia RSA de 2048 bits;

6.3.5. Implementar no mínimo 400 mil conexões SSL simultâneas utilizando criptografia de 2048 bits;

6.3.6. A Solução de visibilidade ofertada deve implementar, no mínimo, os seguintes algoritmos de troca de chaves com autenticação:

6.3.6.1. RSA;

6.3.6.2. DHE;

6.3.6.3. DHE_RSA;

6.3.6.4. ECDHE com PFS (Perfect Forward Secrecy)

6.3.6.5. ECDHE_RSA;

6.3.6.6. ECDHE_ECDSA.

6.3.7. A Solução de visibilidade ofertada deve implementar, no mínimo, os seguintes métodos de autenticação de mensagem:

6.3.7.1. SHA;

6.3.7.2. SHA256;

6.3.7.3. SHA384;

6.3.7.4. POLY1305.

6.3.8. Deverá implementar Host Categorization, permitindo selecionar tráfegos que não serão descriptografados, como dados financeiros por exemplo.

6.3.9. A funcionalidade SSL Decryption se suportar, no mínimo, os seguintes protocolos:

6.3.9.1. SSL 3;

6.3.9.2. TLS 1.0;

6.3.9.3. TLS 1.1;

6.3.9.4. TLS 1.2;

6.3.9.5. TLS 1.3.

6.3.10. Deve suportar chaves de 1024 bits, 2048 bits e 4096 bits.

6.3.11. A Solução de visibilidade ofertada deve suportar, no mínimo, as seguintes cifras de criptografia:

6.3.11.1. AES_128_CBC;

6.3.11.2. AES_256_CBC;

6.3.11.3. AES_256_GCM;

6.3.11.4. CHACAH20;

6.3.11.5. Camellia128;

6.3.11.6. Camellia256;

6.3.11.7. DES_CBC;

6.3.11.8. 3DES_EDE_CBC;

6.3.11.9. SEED;

6.3.11.10. IDEA;

6.3.11.11. Chacah20-Poly1305.

6.4. **ALTA DISPONIBILIDADE**

6.4.1. Quando implementado em alta disponibilidade, em caso de falha de um dos equipamentos, a inspeção SSL deverá ser realizada pelo outro equipamento.

6.4.2. Deve fazer ou permitir a opção de bypass do tráfego caso falhe o TLS handshake.

6.4.3. 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.

6.4.4. 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;

6.4.5. 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.

6.5. **INTERFACES DE COMUNICAÇÃO**

6.5.1. A Solução deverá contemplar 5 (cinco) interfaces padrão Ethernet 100/40Gbps QSFP28.

6.5.2. A Solução deverá contemplar 2 (dois) transceivers 100Gbps QSFP28 de curto alcance, com suas respectivas fibras OM4 UPC de 5,0m. O tipo de conector da fibra será definido durante a fase de implementação da solução.

6.5.3. A Solução deverá contemplar 2 (duas) interfaces padrão Ethernet 100/40Gbps QSFP28, do tipo “bypass”.

6.5.4. A Solução deverá contemplar 16 (dezesseis) interfaces padrão Ethernet 25/10Gbps SFP28.

7. ITEM 06 – SERVIÇO PARA O TRATAMENTO DO TRÁFEGO DE APLICAÇÕES – COMPATÍVEL COM OS SERVIÇOS DO TIPO 1 E 2.

7.1. **CARACTERÍSTICAS TÉCNICAS**

7.1.1. O objeto ofertado deverá corresponder a 1 (um) módulo o qual possibilita a expansão o tratamento do tráfego de aplicações para os equipamentos do Tipo 1 ou 2.

7.1.2. O licenciamento complementar 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.

7.2. **CARACTERÍSTICAS DE DESEMPENHO**

7.2.1. Deverá implementar um throughput exclusivo de tráfego de processamento de filtro de aplicações de, no mínimo, 42 (quarenta e dois) Gbps, respeitando as demais condições técnicas previstas para segurança da informação.

7.3. **CARACTERÍSTICAS DE SEGURANÇA DA INFORMAÇÃO**

7.3.1. Deve gerar, no mínimo, os seguintes metadados para prover informações superiores à da camada de rede, quando utilizando IPFIX/CEF:

7.3.1.1. HTTP Method;

7.3.1.2. HTTP Response Code

7.3.1.3. HTTP Version;

7.3.1.4. HTTP Host;

7.3.1.5. HTTP User Agent;

7.3.1.6. DNS Query Name;

7.3.1.7. DNS Query Type

7.3.1.8. DNS Response Code;

7.3.1.9. DNS Response TTL;

7.3.1.10. DNS Response Name;

7.3.1.11. DNS Response IPv6/IPv4;

7.3.1.12. SSL Certificate Issuer;

7.3.1.13. SSL Certificate CN;

7.3.1.14. SSL Version;

7.3.1.15. SSL Cipher.

7.3.2. 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.

7.3.3. A funcionalidade DPA deve permitir a criação de filtros (regras) utilizando linguagem de programação Perl ou RegEx.

7.3.4. A funcionalidade DPA deve permitir a criação de filtros (regras) utilizando uma string.

7.3.5. 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.

7.3.6. 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.

7.3.7. 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.

7.3.8. 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).

7.3.9. Deve implementar a identificação de, no mínimo, 3500 aplicações agrupadas por famílias ou grupos de aplicações tais como YouTube, Whatsapp e Gmail.

7.3.10. Deve implementar a definição de assinaturas para aplicações customizadas, incluindo protocolos e extensões proprietárias.

7.3.11. Após a identificação do tráfego com base na aplicação, a solução deve suportar a criação de filtros (regras) de encaminhamento e replicação de tráfego.

8. ITEM 07 – SERVIÇO PARA O TRATAMENTO DO TRÁFEGO DE APLICAÇÕES – COMPATÍVEL COM OS SERVIÇOS DO TIPO 3.

8.1. CARACTERÍSTICAS TÉCNICAS

8.1.1. O objeto ofertado deverá corresponder a 1 (um) módulo o qual possibilita a expansão o tratamento do tráfego de aplicações para Solução de visibilidade ofertada Tipo 3.

8.1.2. O licenciamento complementar 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.

8.2. **CARACTERÍSTICAS DE DESEMPENHO**

8.2.1. Deverá implementar um throughput exclusivo de tráfego de processamento de filtro de aplicações de, no mínimo, 132 (cento e trinta e dois) Gbps, respeitando as demais condições técnicas previstas para segurança da informação.

8.3. **CARACTERÍSTICAS DE SEGURANÇA DA INFORMAÇÃO**

8.3.1. Deve gerar, no mínimo, os seguintes metadados para prover informações superiores à da camada de rede, quando utilizando IPFIX/CEF:

8.3.1.1. HTTP Method;

8.3.1.2. HTTP Response Code

8.3.1.3. HTTP Version;

8.3.1.4. HTTP Host;

8.3.1.5. HTTP User Agent;

8.3.1.6. DNS Query Name;

8.3.1.7. DNS Query Type

8.3.1.8. DNS Response Code;

8.3.1.9. DNS Response TTL;

8.3.1.10. DNS Response Name;

8.3.1.11. DNS Response IPv6/IPv4;

8.3.1.12. SSL Certificate Issuer;

8.3.1.13. SSL Certificate CN;

8.3.1.14. SSL Version;

8.3.1.15. SSL Cipher;

8.3.2. Deve suportar a funcionalidade DPA (Deep Packet Analysis), que permita criar filtros (regras) que identifiquem qualquer informação dentro do pacote, desde o cabeçalho até o Payload.

8.3.3. A funcionalidade DPA deve permitir a criação de filtros (regras) utilizando linguagem de programação Perl ou RegEx.

8.3.4. A funcionalidade DPA deve permitir a criação de filtros (regras) utilizando uma string.

8.3.5. 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.

8.3.6. Deve suportar 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.

8.3.7. A funcionalidade App-Aware deve suportar 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.

8.3.8. Deve suportar 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).

8.3.9. Deve suportar a identificação de, no mínimo, 3500 aplicações agrupadas por famílias ou grupos de aplicações tais como YouTube, Whatsapp e Gmail.

8.3.10. Deve suportar a definição de assinaturas para aplicações customizadas, incluindo protocolos e extensões proprietárias.

8.3.11. Após a identificação do tráfego com base na aplicação, a solução deve suportar a criação de filtros (regras) de encaminhamento e replicação de tráfego.

8.4. **INTERFACES DE COMUNICAÇÃO**

8.4.1. A Solução deverá contemplar 8 (oito) interfaces padrão Ethernet 100/40Gbps QSFP28.

8.4.1.1. A Solução deverá contemplar 2 (dois) transceivers 100Gbps QSFP28 de curto alcance, com suas respectivas fibras OM4 UPC de 5,0m. O tipo de conector da fibra será definido durante a fase de implementação da solução

.

9. ITEM 08 – GERENCIAMENTO CENTRALIZADO DA SOLUÇÃO.

9.1. **CARACTERÍSTICAS GERAIS DA PLATAFORMA**

9.1.1. 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.

9.1.2 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.

9.1.3 No caso de fornecimento de plataforma virtualizada:

9.1.3.1 A solução deverá ser compatível com, no mínimo, os hypervisors VMware e Hyper-V.

9.1.3.2 A solução deverá ser fornecida conforme suas quantidades mínimas que garantem a alta disponibilidade do gerenciamento da plataforma.

9.1.3.3 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.

9.1.4 No caso de fornecimento de plataforma física:

9.1.4.1 Os equipamentos físicos, em alta disponibilidade, deverão ser disponibilizados com todos os softwares necessários para prover os requisitos técnicos especificados.

9.1.4.2 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.

9.1.4.3 Cada equipamento deverá possuir altura máxima de 1RU.

9.1.4.4 Todo hardware que compõe a solução deverá possuir alimentação elétrica de 110/240 V, 47 a 63 Hz, com chaveamento automático.

9.1.4.5 Todos os componentes de disponibilidade dos hardwares deverão ser redundantes (exceto por controladoras RAID), e hot-swap (exceto por slots PCIe, processadores e memórias).

9.2. CARACTERÍSTICAS DE GERENCIAMENTO CENTRALIZADO

9.2.1. A Solução deverá contemplar um software capaz de controlar, administrar, gerenciar e monitorar a solução para interceptação do tráfego prevista nesta contratação.

9.2.2 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.

9.2.3 Possuir gerenciador em um único ponto central para orquestrar os elementos físicos e virtuais que compõem a solução de interceptação do tráfego.

9.2.4 A solução deve possuir uma interface gráfica e intuitiva com API abertas para simples customização de aplicações e integração com produtos de terceiros

9.2.5 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.

9.2.6 Possuir interface gráfica para a criação dos filtros (regras), onde é possível selecionar as portas de Rede e as portas de Ferramentas, independentemente da Solução de visibilidade ofertada. Os filtros (regras) criados para estes tráfegos deverão ser aplicados através desta mesma interface Web (HTTPS), facilitando a operação e entendimento dos fluxos.

9.2.7 A solução deve permitir o inventário detalhado de atributos dos ativos da solução, atendendo, no mínimo, números seriais, módulos instalados, status da solução de visibilidade ofertada e versão de software instalado.

9.2.8 A solução deve permitir o armazenamento das configurações dos dispositivos.

9.2.9 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.

9.2.10 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.

9.2.11 A ferramenta deve permitir a execução do reset dos dispositivos.

9.2.12 A ferramenta deve permitir restaurar a configuração armazenada. Deve ser possível ainda aplicar essa configuração em um equipamento em processo de substituição.

9.2.13 Deve permitir a instalação dos TAPs virtuais a partir da console de gerência.

9.2.14 Deve possuir integração via API com a VMWare, para permitir cópia do tráfego entre as VMs mesmo em caso de mobilidade das VMs.

9.2.15 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.

9.2.16 A solução deverá possuir dashboards com, no mínimo, as seguintes informações:

9.2.16.1 Total de portas que estão perdendo pacotes;

9.2.16.2 Total de portas acima do limite de utilização, tanto portas de Rede como portas de Ferramenta;

9.2.16.3 TOP portas com maior utilização;

9.2.16.4 Visualização simplificada de todos os filtros (regras) aplicados, indicando as portas de Redes e Ferramentas;

10. ITEM 09 – SERVIÇO DE INTERCEPTAÇÃO DO TRÁFEGO VIRTUALIZADO ESSENCIAL.

10.1. CARACTERÍSTICAS DE LICENCIAMENTO E FORNECIMENTO

13.1.1. A Solução deverá contemplar no formato de equipamento disponibilizado virtual, com seu licenciamento na modalidade de subscrição.

13.1.2. 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.

13.1.3. A solução entregue deverá estar licenciada para processar, no mínimo, 50 TB (cinquenta terabytes) de dados por dia.

10.2. CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO

10.2.1. Deverá implementar a coleta de tráfego dentro do mundo virtual (tráfego entre VMs) através de Interceptadores Virtualizados ou Virtual TAPs.

10.2.2. Deverá se integrar, através de APIs específicas, com a VMware, OpenStack ou Nutanix, não sendo aceitas soluções que utilizem do modo promíscuo ou que façam qualquer alteração no kernel do Hypervisor, para todas as plataformas solicitadas.

10.2.3. Para a coleta de tráfego entre VMs deverá ser compatível com, no mínimo, as seguintes plataformas:

10.2.3.1. VMware 6.7 ou superior;

10.2.3.2. NSX-T 3.1 ou superior; OpenStack;

10.2.4. Deverá suportar o monitoramento de múltiplos switches virtuais distribuídos da VMware simultaneamente.

10.2.5. 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.

10.2.6. 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.

10.2.7. Deve implementar a coleta de tráfego entre VMs de, no mínimo, 1.000 hypervisors e integração com, no mínimo, 10 vCenters.

10.2.8. Deverá permitir a visualização e monitoramento, através de um gerencia centralizada, de todos os equipamentos disponibilizados virtuais componentes da solução.

10.2.9. Deverá implementar a coleta de tráfego dentro do ambiente de conteinerização (Kubernetes) através de Container TAPs.

10.2.10. Deverá coletar o tráfego no ambiente de conteinerização independente da camada de rede de contêineres (CNI) utilizada.

10.2.11. Deverá coletar o tráfego de forma independente dos PODs em execução, não sendo necessária instrumentação dos PODs das aplicações.

10.2.12. Para coleta de tráfego entre PODs deverá ser compatível com, no mínimo, as seguintes plataformas:

10.2.12.1. Amazon Elastic Kubernetes Services (EKS);

10.2.12.2. Azure Kubernetes Services (AKS);

10.2.12.3. VMWare Tanzu;

10.2.12.4. Redhat Openshift;

10.2.12.5. Kubernetes nativo.

10.2.13. 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.

10.2.14. Deverá suportar a captura de tráfego dos PODs antes da encriptação e após a decriptação, eliminando a necessidade de posicionamento de soluções de decriptação do tipo Man-in-the-Middle (MiTM). Deverá permitir a seleção de quais PODs serão monitorados baseado em atributos do próprio ambiente de conteinerização, tais como:

10.2.14.1. Namespaces;

10.2.14.2. Nomes dos serviços;

10.2.14.3. Nomes dos PODs.

10.2.15. 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:

10.2.15.1. Windows Server 2012 ou superior;

10.2.15.2. Windows 10 ou superior.

10.2.15.3. Distribuições Linux baseadas:

10.2.15.3.1. Redhat/CentOS/Fedora versões 7.5 ou superior;

10.2.15.3.2. Ubuntu/Debian versões 18-04 ou superior;

10.2.15.3.3. Amazon Linux versões 1 e 2.

10.2.16. Deverá permitir a pré-filtragem do tráfego nos TAPs virtuais antes de enviá-lo para as ferramentas de segurança.

10.2.17. Deverá permitir a coleta de tráfego em ambientes de nuvem, tais como AWS, Azure e GCP.

10.2.18. Deverá permitir a visualização e monitoramento da taxa de tráfego e o resumo do volume de tráfego agregado.

10.2.19. Deve implementar a funcionalidade de desencapsulamento de cabeçalhos L2GRE, VXLAN, ERSPAN e GENEVE dos pacotes de rede.

10.2.20. 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, no ambiente virtual.

10.2.21. Deve implementar a funcionalidade de mascaramento de dados nos pacotes para garantir a privacidade de dados.

10.2.22. Deve implementar a funcionalidade de slicing (corte) dos pacotes, reduzindo o volume de tráfego com payloads irrelevantes.

10.2.23. Deve implementar o balanceamento de carga do tráfego para dois túneis L2GRE ou VXLAN diferentes, permitindo que sejam utilizadas ferramentas de monitoramento redundantes.

11. ITEM 10 - SERVIÇO DE INTERCEPTAÇÃO DO TRÁFEGO VIRTUALIZADO AVANÇADO.

11.1. CARACTERÍSTICAS DE LICENCIAMENTO E FORNECIMENTO

11.1.1. A Solução deverá contemplar no formato de equipamento disponibilizado virtual, com seu licenciamento na modalidade de subscrição.

11.1.2. 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.

11.1.3. A solução entregue deverá estar licenciada para processar, no mínimo, 50 TB (cinquenta terabytes) de dados por dia.

11.2. CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO

11.2.1. Deverá fornecer e permitir a execução de todas as funcionalidades descritas no Interceptador de Tráfego Virtualizado Essencial e, complementarmente, implementar as seguintes tecnologias:

11.2.1.1. Deve implementar a filtragem do tráfego de rede baseado em aplicações (camada 7).

11.2.1.2. 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.

11.2.1.3. Deve permitir que a base de aplicações seja atualizada periodicamente.

11.2.1.4. Deve enriquecer as informações de NetFlow com dados contextuais da camada de aplicação.

11.2.1.5. Deve implementar a extração de metadados do tráfego para mais de 3000 aplicações diferentes.

11.2.1.6. Deve extrair mais de 5000 atributos das diferentes aplicações.

11.2.1.7. Deve permitir o envio de metadados dados para até quatro coletores diferentes.

11.2.1.8. Deve implementar o envio de dados em diferentes formatos, tais como IPFIX, CEF e JSON sobre HTTPS.

11.2.1.9. Deve suportar a decriptação passiva (out-of-band) do tráfego TLS.

11.2.1.10. Deve implementar a captura de pacotes antes da criptografia e após a decriptação, no mínimo para os seguintes sistemas operacionais e ambientes de conteinerização:

11.2.1.10.1. Sistemas Linux: 14.2.1.10.1.1. Baseados em Debian;

14.2.1.10.1.2. Baseados em Redhat.

11.2.1.10.2. Ambientes Kubernetes:

11.2.1.10.2.1. AKS;

11.2.1.10.2.2. EKS;

11.2.1.10.2.3. Openshift;

11.2.1.10.2.4. Tanzu.

11.2.1.11. Deve implementar a abertura das seguintes variações de criptografias do TLS:

14.2.1.11.1. TLS 1.2 com PFS (Perfect Forward Secrecy);

14.2.1.11.2. TLS 1.3;

14.2.1.11.3. mTLS.

11.2.1.12. A funcionalidade deve ser independente de upgrades do S.O.

11.2.1.13. Deve implementar IPv4 e IPv6.

11.2.1.14. Deve implementar a biblioteca OpenSSL, no mínimo, nas seguintes versões:

14.2.1.14.1. 1.0.2;

14.2.1.14.2. 1.1.0;

14.2.1.14.3. 1.1.1;

14.2.1.14.4. 3.x.

11.2.2. Deve implementar a funcionalidade Packet De-Duplication (Deduplicação de Pacotes), enviando somente uma única cópia do pacote para as Ferramentas de monitoramento, no ambiente virtual.

11.2.3. Deve implementar a geração de Netflow, trazendo visibilidade de 100% do tráfego.

12. ITEM 11 – SERVIÇO CENTRALIZADO DE CHASSI PARA INTERCONECTOR PASSIVO DE INTERCEPTAÇÃO DO TRÁFEGO - INTERFACES ÓPTICAS

12.1. CARACTERÍSTICAS TÉCNICAS

12.1.1. Deve ser composto por uma única solução com um único equipamento disponibilizado, montável em rack 19” devendo este vir acompanhado dos devidos acessórios para tal equipamento, deverá ser do tipo chassis/em módulo.

12.1.2. Deve possuir altura máxima de 1 (um) rack unit.

12.1.3. Operar em temperaturas de 0ºC a 60ºC e umidade relativa de 10% a 85%.

12.1.4. Deve ser totalmente passivo, ou seja, não é necessário nenhum tipo de alimentação elétrica, software e configuração para o seu funcionamento.

12.1.5. O chassi deverá permitir a acomodação dos Interconectores Passivos de Interceptação do Tráfego, seja para aqueles com interfaces SFP ou para aqueles com interfaces QSFP.

13. ITEM 12 – SERVIÇO DE INTERCONECTOR PASSIVO DE INTERCEPTAÇÃO DO TRÁFEGO – INTERFACES SFP

13.1. **CARACTERÍSTICAS TÉCNICAS**

13.1.1. Deverá ser compatível com o Chassi para Interconector Passivo de Interceptação do Tráfego.

13.1.2. O Interconector Passivo deverá possuir as seguintes características de interfaces, fibras, conectores e Split Ratio:

13.1.2.1. Possuir 2 (duas) interfaces de rede, responsável por conectar os dispositivos de rede;

13.1.2.2. 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;

13.1.3. 3. A Solução deverá contemplar, 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.

14. ITEM 13 – SERVIÇO DE INTERCONECTOR PASSIVO DE INTERCEPTAÇÃO DO TRÁFEGO – INTERFACES QSFP

14.1. **CARACTERÍSTICAS TÉCNICAS**

14.1.1. Deverá ser compatível com o Chassi para Interconector Passivo de Interceptação do Tráfego.

14.1.2. O Interconector Passivo deverá possuir as seguintes características de interfaces, fibras, conectores e Split Ratio:

14.1.2.1. Possuir 2 (duas) interfaces de rede, responsável por conectar os dispositivos de rede;

14.1.2.2. 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;

14.1.3. A Solução deverá contemplar, 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.

15. ITEM 14 – SERVIÇO DE INTERCONECTOR PASSIVO DE INTERCEPTAÇÃO DO TRÁFEGO – INTERFACES RJ-45

15.1. CARACTERÍSTICAS TÉCNICAS

15.1.1. O Interconector Passivo deverá possuir os seguintes requisitos técnicos:

15.1.1.1 Deve ser composto por um único equipamento, montável em rack 19" devendo este vir acompanhado dos devidos acessórios para tal equipamento, deverá ser do tipo chassis/em módulo.

15.1.1.2 Deve possuir altura máxima de 1 (um) rack unit.

15.1.2 Deverá suportar as seguintes características:

15.1.2.1 Possuir 2 (duas) interfaces de rede, responsável por conectar os dispositivos de rede;

15.1.2.2 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;

15.1.2.3 A Solução deverá contemplar, no mínimo, 4 (quatro) Interconectores Passivos ou TAPs, para interceptar enlaces UTP.

16. ITEM 15 – SERVIÇO DE CONCENTRADOR DE TRÁFEGO DE SEGURANÇA.

16.1 CARACTERÍSTICAS TÉCNICAS

16.2 A Solução deverá contemplar as licenças necessárias para ativação de todas as suas portas e demais funcionalidades aqui solicitadas.

16.3 A Solução de visibilidade ofertada deverá, majoritariamente, ser interligado a ao menos 1 (um) dos Equipamentos Interceptadores de Tráfego Tipo 1, 2 ou 3.

16.4 Deverá ser compatível com transceivers SFP, SFP+, QSFP+ e QSFP28.

16.5 A Solução de visibilidade ofertada deverá possuir, no mínimo, 1 (um) rack unit.

16.6 A Solução de visibilidade ofertada deverá possuir, no mínimo, 2 (duas) fontes de alimentação 100-240 VAC.

16.7 CARACTERÍSTICAS FUNCIONAIS

16.7.1 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.

16.7.2 Deverá possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas de “Rede”, “Rede Inline”, “hibrida”, “circuito”, “Ferramenta” e portas de “Ferramenta Inline”.

16.7.3 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.

16.7.4 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 aos Equipamentos Tipo 1, 2 ou 3.

16.7.5 Entende-se por portas de Rede Inline, todas as portas que serão responsáveis por se conectar de forma Inline a rede de produção.

16.7.6 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 aos Equipamentos Tipo 1, 2 ou 3.

16.8 GERENCIAMENTO DO CONCENTRADOR

16.8.1 O concentrador deve possuir uma interface gráfica e intuitiva com API abertas para simples customização de aplicações e integração com produtos de terceiros.

16.8.2 Deverá permitir configuração customizada baseadas nos perfis de acesso (RBAC - Role Base Access Control).

16.8.3 Deverá implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.

16.8.4 Deverá possuir suporte a MIB II.

16.8.5 Deverá implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.

16.8.6 Deverá suportar SNMP trap sobre IPv6.

16.8.7 Deverá permitir a atualização remota do sistema operacional e arquivos de configuração utilizados na Solução de visibilidade ofertada, via interface de gerenciamento.

16.8.8 Deverá permitir a gravação de log externo (syslog).

16.8.9 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

16.8.10 Deverá possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como estatísticas de utilização e log de eventos.

16.8.11 Deve possuir gerenciamento através de interface Web (HTTPS) e CLI.

16.8.12 Deverá implementar o protocolo NTP (Network Time Protocol).

16.8.13 Deverá implementar mecanismo de autenticação para acesso local ou remoto da Solução de visibilidade ofertada baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+, RADIUS e LDAP.

16.8.14 Deve suportar IPv6 para TACACS+.

16.8.15 Deverá implementar o protocolo SSHv2 para acesso à interface de linha de comando.

16.8.16 Deverá proteger a interface de comando da Solução de visibilidade ofertada através de senha.

16.9 INTERFACES DE COMUNICAÇÃO

16.2.17. A Solução deverá contemplar (48) portas de 1/10/25Gbps compatíveis com os padrões SFP.

16.2.18. A Solução deverá contemplar 8 (oito) portas de 40/100Gbps compatíveis com os padrões QSFP.

17 ITEM 16 – SERVIÇOS DE TRANSCEIVER TIPO 1 – 1 GBPS ETHERNET

17.1 A Solução deverá contemplar 1 (um) Transceivers 1 Gbps compatível com os equipamentos interceptadores de tráfego, tipos 1, 2 ou 3.

17.2 Deverá ser do padrão SFP e possuir conector do tipo RJ-45.

17.3 Deverá ser hot-swap, permitindo a sua remoção mesmo com o equipamento ou módulo energizado.

17.4 Deverá ser propício para a transmissão de dados em curto alcance, permitindo atingir, no mínimo, 30 (trinta) metros de distância.

17.5 A Solução deverá contemplar cabos UTP, com conectores RJ-45. A metragem dos cabos será definida durante a fase de implantação da solução.

18 ITEM 17 – SERVIÇOS DE TRANSCEIVER TIPO 2 – 10 GBPS ETHERNET

18.1 A Solução deverá contemplar 1 (um) Transceivers 10Gbps compatível com os equipamentos interceptadores de tráfego, tipos 1, 2 ou 3.

18.2 Deverá ser do padrão SFP+ e possuir conector do tipo LC.

18.3 Deverá ser hot-swap, permitindo a sua remoção mesmo com equipamento ou módulo energizado.

18.4 Deverá ser propício para a transmissão de dados em curto alcance, permitindo atingir, no mínimo, 50 (cinquenta) metros de distância.

18.5 A Solução deverá contemplar fibras OM4 UPC, com conectores LC. A metragem das fibras será definida durante a fase de implantação da solução.

19 ITEM 18 – SERVIÇOS DE TRANSCEIVER TIPO 3 – 25G BPS ETHERNET

19.1 A Solução deverá contemplar 1 (um) Transceivers 25Gbps compatível com os equipamentos interceptadores de tráfego, tipos 1, 2 ou 3.

19.2 Deverá ser do padrão SFP28 e possuir conector do tipo LC.

19.3 Deverá ser hot-swap, permitindo a sua remoção mesmo com o equipamento ou módulo energizado.

19.4 Deverá ser propício para a transmissão de dados em curto alcance, permitindo atingir, no mínimo, 50 (cinquenta) metros de distância.

19.5 A Solução deverá contemplar fibras OM4 UPC, com conectores LC. A metragem das fibras será definida durante a fase de implantação da solução.

20 ITEM 19 – SERVIÇOS DE TRANSCEIVER TIPO 4 – 40 GBPS ETHERNET

20.1 A Solução deverá contemplar 1 (um) Transceivers 40Gbps compatível com os equipamentos interceptadores de tráfego, tipos 1, 2 ou 3.

20.2 Deverá ser do padrão QSFP+.

20.3 Deverá ser hot-swap, permitindo a sua remoção mesmo com o equipamento ou módulo energizado.

20.4 Deverá ser propício para a transmissão de dados em curto alcance, permitindo atingir, no mínimo, 50 (cinquenta) metros de distância.

20.5 A Solução deverá contemplar 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.

21 ITEM 20 – SERVIÇOS DE TRANSCEIVER TIPO 5 – 100 GBPS ETHERNET

21.1 A Solução deverá contemplar 1 (um) Transceivers 100Gbps compatível com os equipamentos interceptadores de tráfego, tipos 1, 2 ou 3.

21.2 Deverá ser do padrão QSFP28.

21.3 Deverá ser hot-swap, permitindo a sua remoção mesmo com a Solução de visibilidade ofertada ou módulo energizado.

21.4 Deverá ser propício para a transmissão de dados em curto alcance, permitindo atingir, no mínimo, 50 (cinquenta) metros de distância.

21.5 A Solução deverá contemplar 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.

22 ITEM 21 – SERVIÇOS DE CONSULTORIA

22.1 SERVIÇOS DE OPERAÇÃO ASSISTIDA E AJUSTE FINO PARA AS SOLUÇÕES DE NPB

22.1.1 O modelo de metrificação adotado não se caracteriza como alocação de posto de trabalho, e sim como prestação de serviço por meio da execução de atividades necessária à customização da solução, como por exemplo customização de relatórios específicos não contemplados no template da ferramenta, sendo essa mensuração estimada com base no Tempo/Esforço e Complexidade.

22.1.2 a emissão de cada OS deve ser feita considerando as atividades que são pertinentes para cada projeto e seu custo em UST.

22.1.3 A CONTRATADA é responsável pela prestação dos serviços caracterizados nas Ordens de Serviço, devendo utilizar o pessoal técnico qualificado na quantidade adequada para garantir a plena qualidade dos produtos entregues, ficando sob sua definição qualquer composição de recursos, otimização de rotinas ou procedimentos.

22.1.4 A CONTRATANTE, para efeito de pagamento, não contabilizará simplesmente as horas utilizadas, mas tão somente os serviços/atividades constantes na OS, devidamente entregues e aceitos.

A identificação e a priorização dos serviços a serem executados serão realizadas pela CONTRATANTE em conjunto com a CONTRATADA.

ANEXO B - CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS DE SOLUÇÃO DE VISIBILIDADE E DETECÇÃO DE AMEAÇAS DO TRÁFEGO DE REDE E SSL DECRYPTION UNIVERSAL COM GERÊNCIA EM NUVEM - INSTALAÇÃO CONFIGURAÇÃO E TESTES (ITENS 1 A 21).

1. PLANEJAMENTO:

1.1 Reunião de Kick-off – Deve ser realizada em duas etapas: a primeira com a equipe de implementação, abordando aspectos técnicos, integração, comunicação, e a segunda com o cliente tratando as formas de acompanhamento ao longo do projeto e prazo;
1.2 Visão geral do projeto, a fim de alinhar os objetivos e metas técnicas;
1.3 Escopo do Projeto;
1.4 Principais Entregas;
1.5 Limites do Projeto;
1.6 Possíveis riscos que podem ocorrer, bem como um plano de prevenção e/ou recuperação;
1.7 Equipe de execução do Projeto;
1.8 Prioridade do Projeto;
1.9 Cronograma do Projeto;
1.10 Esclarecimento de dúvidas;
1.11 Reunião de Follow-up – Deve ser realizada pelo menos uma vez por semana durante o período de implementação do projeto. Poderá ser feita de forma remota;
1.12 Relato breve quantificando do status das principais atividades do projeto;
1.13 Apresentação de fatos e informações relevantes que permitam análise e acompanhamento do andamento do projeto;
1.14 Avaliação de possíveis sanções que poderão ser aplicadas caso ocorram atrasos ou imprevistos no projeto, especialmente as que envolvem qualidade do trabalho, cronograma e custos;
1.15 Reunião EndUp – Deve ser uma reunião formal a ser realizada ao término de todas as atividades do projeto, com a presença do cliente, gerente do projeto e equipe do projeto;
1.16 Descrição resumida do projeto, desde seu início até sua finalização;
1.17 Síntese das fases e marcos principais e caracterização do cumprimento de tudo que ficou acertado e aceito pelo cliente em cada fase;
1.18 Certificação de que o projeto que está sendo entregue neste momento cumpre todos os requisitos acordados no início, e/ou modificados e redimensionados pelas partes ao longo dos trabalhos;
1.19 Entrega formal da documentação resultante da implementação do projeto;

2. IMPLANTAÇÃO:

2.1 Os serviços deverão ser executados na sua totalidade pela CONTRATADA e deverão obrigatoriamente ter o acompanhamento da equipe técnica da CONTRATANTE;
2.2 O escopo de implementação, migração de serviços, configuração de políticas e funcionalidades para os produtos deste termo de referência, contempla configurações lógicas e testes na sede da CONTRATANTE;
2.3 A instalação deverá ser executada no local definido pelo CONTRATANTE, mediante prévio agendamento e em acordo com o cronograma;
2.4 Em até 30 (trinta) dias corridos da assinatura do Contrato, a CONTRATADA deverá submeter a verificação e aprovação pela área Técnica de TI da CONTRATANTE o plano completo, mencionado neste Termo.
2.5 Os produtos e soluções terão como prazo de entrega um período de 60 dias corridos a partir da data de emissão da ordem de compra ou execução.

3. RECURSOS:

3.1 Os recursos humanos a serem alocados pela CONTRATADA, suas qualificações mínimas e os seus respectivos papéis e responsabilidades no projeto:
3.1.1 Gerente de Projetos – Caberá a ele a liderança da equipe de projeto e as atividades de gerenciamento e facilitação para o alcance dos objetivos do projeto segundo as melhores práticas de mercado.
3.1.2 Analista (s) Integrador (es) – conjunto com um ou mais profissionais que (individualmente ou conjuntamente):
3.1.2.1 3.2 Caberá a este(s) profissional(ais) da equipe, o desenvolvimento do projeto de arquitetura futura, a execução e coordenação de atividades de migração, implantação, instalação, configuração e testes e outras atividades técnicas conforme as prescrições deste edital.

ANEXO C - MANUTENÇÃO E SUPORTE TÉCNICO

1. A CONTRATADA dará suporte e assistência técnica 24X7 conforme descrito abaixo caso um dos itens 1 a 24 seja contratado:
2. A CONTRATADA será responsável pela administração e manutenção do serviço em regime de 24x7 para atendimentos remotos e o regime 8x5 suporte técnico especializado de 2° (segundo nível) poderá ser presencial ou remoto, durante todo o período do serviço comtemplado nesse Edital. As tarefas atinentes ao transporte, deslocamento e remessa necessários, seja na implementação, substituição e/ ou remoção de equipamentos defeituosos será de responsabilidade da CONTRATADA.
3. Para garantir a qualidade e disponibilidade do serviço, deverá ser disponibilizada pela empresa CONTRATADA uma ferramenta de monitoramento com estrutura dedicada
4. A ferramenta deve ser acompanhada de todos os itens necessários para operacionalização, tais como softwares de apoio (sistema operacional, etc) e licenças de softwares;
5. O serviço de monitoramento 24x7 deverá ser prestado OBRIGATÓRIA E INDISPENSAVELMENTE através de NOCs (Network Operation Center) redundantes da empresa CONTRATADA que já deverão estar em pleno funcionamento até a data da assinatura do Contrato. Será o ponto único de contato com a equipe técnica da CONTRATANTE para abertura de chamados, incidentes, problemas, dúvidas e requisições relacionadas aos serviços contratados, atuando como a primeira instância de atendimento à CONTRATANTE.
6. Os serviços prestados pelo NOC compreendem, entre outros, os seguintes procedimentos:
6.1. Monitoramento pró-ativo do ambiente de rede WAN do CONTRATANTE;
6.2. Suporte técnico para identificação e resolução de problemas em software e nos equipamentos;
6.3. Resolução de problemas quanto acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;
6.4. Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;
6.5 Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;
6.5. Suporte à criação, geração e parametrização de relatórios e eventos de segurança de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;
7. Encaminhar incidentes aos gestores do fabricante da solução, para suas providências;
8. Suporte em demais configurações de segurança, redundância e gerência;
9. Encaminhamento para o Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;
10. Apoio técnico para tarefas de auditoria e análise de logs.
11. A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio da uma solução de contorno ou definitiva. Ainda caberá à CONTRATADA agir de forma proativa aplicando medidas para a boa manutenção afim de garantir a regularidade da operação do serviço.
12. O atendimento e suporte técnico especializado de 1° (primeiro nível) será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, controle dos Indicadores de monitoramento, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.
13. O atendimento e suporte técnico especializado de 2° (segundo nível) em regime 8x5, poderá ser remoto ou presencial, caso o suporte remoto não seja suficiente para resolução do problema e será responsável pela prevenção e resolução de incidentes, problemas e requisições, identificando a causa raiz de eventual problema e buscando sua solução, além da execução de atividades remotas e/ou presenciais em incidentes, solicitações de maior complexidade.

14. Os Técnicos deverão ser capacitados e certificados para prestação dos serviços, resolução de incidentes, problemas e solicitações nos equipamentos ofertados. O comparecimento de um técnico ao local da necessidade será de no máximo 48 (quarenta e oito) horas para atendimentos na área que abrange e define a Região Metropolitana da Capital e de até 5 (cinco) dias para as outras demais localidades (interior do Estado) e devendo sempre atender aos critérios de SLA determinados nesse Edital.
15. Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), e/ou serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAS. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.
16. A atualização de firmware quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.
17. A CONTRATADA deverá fornecer informações de monitoramento on-line, via dashboard que permita o acompanhamento em tempo real do estado dos ativos. Deverá ainda apresentar relatórios mensais, por meio digital (DOCX, XLSX ou PDF), com o diagnóstico e controle dos equipamentos monitorados (dados, informações, descrição, indicadores e métricas que permitam quantificar o desempenho e a disponibilidade da ope- ração do serviço).
18. A CONTRATADA deverá disponibilizar uma ferramenta de Service Desk comprovadamente aderente as boas práticas do ITIL e que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipa- mentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).
19. Os relatórios de chamados abertos poderão ser solicitados a qualquer instante pela CONTRATANTE dentro das condições estipuladas, respeitando, no entanto, um prazo de até 48 (quarenta e oito) horas uteis. Esses relatórios deverão ser retidos pelo tempo mínimo equivalente a vigência do contrato e após o seu encerramento inutilizados.
20. A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.
21. A CONTRATANTE deverá definir pessoas do seu Quadro de Funcionários que terão acesso de Administração nos equipamentos disponibilizados e essas pessoas deverão comunicar à empresa CONTRATADA qualquer alteração de configuração realizada nos equipamentos fornecidos nessa contratação e nessa situação respondendo por sua conta e risco pelas intervenções que possam ter efetuado.
22. A CONTRATADA deverá respeitar os tempos máximos de ATENDIMENTOS e SLA (Nível de Acordo de Serviço) abaixo descritos, sob a pena de multa no caso de falhas em seu integral cumprimento:
23. Operação parada (incidente que gere parada total de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 2 (duas) horas.
24. Operação impactada (incidente que gere parada parcial de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 4 (quatro) horas.
25. Requisição de serviço (solicitações de mudanças nos equipamentos ou serviços do contrato) o tempo de atendimento será de até 8 (oito) horas.
26. Informações de contrato (solicitação de informação, parecer ou relatório de algum serviço contemplado no contrato) o tempo de atendimento será de até 12 (doze) horas.

ANEXO D - CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS

1. DA COMPLEXIDADE DO SERVIÇO

1.1. A adoção do valor de referência único facilita à contabilização dos serviços, todavia, demanda a definição dos parâmetros relativos a ponderação aplicável ao dimensionamento do serviço; nesse sentido, para efeito de cada projeto a ser contratado, serão adotados os seguintes pesos de complexidade:

Complexidade	Serviços	Peso Complexidade
Baixa	**Monitoramento de chamados de terceiros. Atendimento aos usuários na modalidade emergencial. Assistência técnica remota (plantão). Atividades de apoio à: monitoramento de ações, acompanhamento de atividades, registros em sistemas básicos, formatação de artefatos básicos de projetos de sistemas, prototipação e atividades similares.**	1,00
Intermediária	**Assistência Técnica Presencial. Análise e levantamento de processos. Criação e implantação da base de conhecimento na solução de gerenciamento de serviços e atualização dos scripts de atendimento. Operação de sistemas complexos, apoiar na criação de artefatos de projetos, especificação casos de uso, regras de negócio, elaboração de diagramas de processos e estratégia, atendimento a demanda de média complexidade de clientes internos, mapeamento de processos e atividades similares.**	1,05
Alta	**Automação de processos na solução de gerenciamento de serviços. Desenvolvimento de painel de controle (dashboards), portfólio e catálogo de serviços. Desenvolvimento de novos relatórios. Implantação de novos processos, apoio na criação e desenvolvimento de projetos, estudos de viabilidade de projetos, criação de novos processos, desenvolvimento de novos sistemas, aperfeiçoamento de processos de gestão do cliente final ou Etice, apoio na implantação de novos sistemas no cliente final ou Etice, e atividades similares.**	1,10
Especialista	**Customização na solução de gerenciamento de serviços. Execução de demanda eventual ou projeto não contemplado dos demais itens em razão de sua necessidade pontual de execução que requeiram conhecimento técnico em áreas correlatas sejam infraestrutura, sistemas, segurança da informação ou atividades similares.**	1,15

2. DO CATÁLOGO DE SERVIÇOS

2.1. Conforme o ITIL, o Catálogo de serviço é um conjunto de informações sobre os serviços de TIC disponíveis para uso, trata-se de um conteúdo dinâmico, que requer revisão e alterações periódicas para que esteja adequado a realidade da TI, demandando assim um processo específico de gerenciamento, para que possa ser atual e aderente.

2.2. No contexto da presente especificação técnica, buscou-se a elaboração de um catálogo que permitisse atender uma vasta gama de necessidades relativas a serviços em nuvem, todavia, conforme as melhores práticas de gerenciamento de serviços e frameworks de mercado a exemplo do ITIL e COBIT o catálogo de serviços por tratar-se de um conteúdo dinâmico, necessita de revisões e adequações que venham a ser necessárias com vistas a assegurar sua aderência ao negócio. Assim com vistas a assegurar a aplicação das boas práticas de forma a suportar adequadamente as necessidades de negócio o catálogo de serviços que integra o presente instrumento estará sujeito a melhorias para a realização do objeto ajustado a realidade da Etice e dos seus clientes finais.

2.3. Em função da evolução da maturidade da Etice e em função da dinâmica dos processos, a versão inicial do catálogo de serviços poderá sofrer revisões com vistas a se adequar a realidade da Etice e de seus clientes finais na ocasião, através de projetos específicos para revisão do catálogo de serviços.
2.4. A versão inicial do Catálogo de Serviços - (ANEXO E) elenca os tipos de solicitações contempladas pelo objeto do serviço, fornecendo referência a parâmetros que definem a ponderação do serviço.

3. DAS CONDIÇÕES DE EXECUÇÃO

3.1. O objeto desta especificação técnica tem por escopo serviços de natureza contínua, prestados sob demanda, para operacionalização de processos descritos no catálogo de serviços, assim como serviços pontuais, prestados sob demanda para a execução de projetos, que venham a ser necessários a efetivação dos objetivos estratégicos da Etice e seus cliente finais no que dependam da tecnologia da informação e comunicação usando ambiente de nuvens.
3.2. A Etice poderá a seu critério utilizar as USTs contratadas para a execução de serviços continuados (processos) ou pontuais (projetos) sem ônus ao objeto contratual, considerando especificações do catálogo de serviços.

4. DA SOLICITAÇÃO DE SERVIÇOS

4.1. Mensalmente ou em caso de necessidade serão abertas ordens de serviço, com os Serviços Técnicos devidamente identificados e associados a uma estimativa (UST) relacionadas aos serviços a serem executados.
4.2. A partir da abertura da OS, todas as atividades necessárias para a execução dos serviços deverão estar relacionadas às demandas devidamente registradas em ferramenta de Gestão de Demandas. Quando não houver disponibilidade desta ferramenta, poderá ser realizada por qualquer outra compatível.
4.3. Para o encerramento de uma demanda é necessário o registro das atividades que evidenciam o seu atendimento.
4.4. O cálculo do número de USTs relativas aos serviços solicitados, será realizado por ocasião da emissão da ordem de serviços (OS) que poderá contemplar a execução de um ou mais serviço. Esse agrupamento só deverá ser aplicado para serviços com durações semelhantes, para não ocasionar retardo no encerramento da OS. O referido cálculo deverá ser feito para cada serviço solicitado na OS conforme a seguinte fórmula:

UST= (Esforço x complexidade)

onde:
UST: corresponde ao quantitativo de unidades de serviços técnicos estimados para a realização do serviço.
Esforço: Somatório da estimativa de todos os esforços decorrentes da alocação temporal de um ou mais recursos necessários ao serviço, considerados os pesos aplicados a cada recurso. Ou seja, Esforço = Fator * Número de horas alocadas.
Complexidade: peso quanto ao tipo predominante de atividades inerentes a sua realização do serviço

4.5. Para aplicação da fórmula da UST ajustada por serviço, deve-se considerar que:
4.5.1. O dimensionamento do esforço para o serviço demandará estudo para definição de estimativas da alocação recursos necessários ao serviço, considerando quantitativos e a alocação temporal dos recursos para atendimento demanda.
4.5.2. A CONTRATADA poderá adotar o fator médio de 1,368 do ANEXO F para dimensionar o esforço;
4.6. Caso opte por não usar o fator médio a CONTRATADA deverá dimensionar o esforço adotando os pesos definidos no ANEXO F – LISTA DE PERFIS TÉCNICOS dos recursos;

5. DO CANCELAMENTO DOS SERVIÇOS

5.1. Nos casos em que a demanda for cancelada por solicitação do cliente final ou da Etice, o trabalho já executado deverá ser medido, avaliado e pago.
5.2. Quando do cancelamento do serviço, a CONTRATADA deverá entregar os produtos do serviço executado, imediatamente, mesmo que inacabados.

5.3. O pagamento dos serviços cancelados está vinculado à entrega dos produtos parciais elaborados pela CONTRATADA até o momento do cancelamento.

ANEXO E - CATÁLOGO DE SERVIÇOS

O catálogo de serviços apresentado na tabela abaixo lista as complexidades esperadas para cada serviço a ser executado.

Este catálogo pode ser alterado pontualmente na medição de serviços no caso de ser detectado pela CONTRATADA e aprovado pelo CONTRATANTE que o serviço apresenta para uma determinada atividade uma complexidade diferente da listada.

Este catálogo pode ser alterado continuamente no caso de ser detectado pela CONTRATADA e aprovado pelo CONTRATANTE que o serviço apresenta para a maioria das atividades relacionadas a ele uma complexidade diferente da listada.

SERVIÇO	COMPLEXIDADE
Avaliação e descoberta de portfólio de aplicações e suasinterdependências para construção de plano para migração.	Intermediário
Avaliação de infraestrutura existente para dimensionamento deinfraestrutura necessária em ambiente de nuvem.	Intermediário
Migração de cargas de trabalho entre sistemas operacionais(Linux/ Windows)	Intermediário
Migração cargas de trabalho entre bancos de dados d e heterogêneos.	Alta
Migração de bases de dados on-premises para nuvem, com ou sem atualização de versão, para: outros motores suportados; bases de dados para propósitos específicos (NoSQL).	Alta
Migração de containers on-premises para soluções de orquestração e repositório de containers gerenciados.	Alta
Migração de cargas de trabalho, elegíveis, de máquinas virtuaispara containers.	Alta
Migração de cargas de trabalho, elegíveis, máquinas virtuais oucontainers para modelo sem servidor.	Alta
Migração de cargas de trabalho em máquinas virtuais paraserviços gerenciados e não gerenciados elegíveis.	Alta
Implementação de mecanismo de alta disponibilidade, escalabilidade horizontal automatizada, monitoramento, verificações de saúde e balanceamento de carga.	Alta

Construção de data warehouse e/ou datamarts a partir de uma ou mais fontes de dados, escalabilidade vertical e horizontal e otimizações de consultas	Especialista
Construção de soluções de analytics a partir de uma ou mais fontes de dados, escalabilidade vertical e horizontal e otimizações de consultas	Especialista
Construção de soluções de Big Data a partir de uma ou mais fontes de dados, escalabilidade vertical e horizontal e otimizações de consultas	Especialista
Desenvolvimento e implementação de projetos que envolvem tecnologias de Inteligência Artificial, linguagens e aprendizado de máquina, redes neurais, preditivas e demais tecnologiasenvolvidas.	Especialista
Desenvolvimento e implementação de projetos de atendimento virtual, robôs e demais ferramentas de conversação inteligente automatizada.	Especialista
Desenvolvimento e implementação de projetos que envolvemsoluções de IoT (Internet das Coisas).	Especialista
Implementação de rede de entrega de conteúdo para conteúdo(site) estáticos.	Intermediário
Criação/configuração de topologia de redes interconectadas com isolamento, firewall, ACL's (Access Control Lists) e auditoria.	Intermediário
Implementação e configuração de conectividade do ambienteon-premises com ambiente em nuvem.	Intermediário
Configuração de serviço de DNS, público ou privado, eintegração com serviço de DNS on-premises.	Intermediário
Implementação de modelo de categorização de custos combase em rótulos, orçamentos e alarmes de consumo mensal.	Baixa
Implementação de controles para filtro de requisições Webclassificadas como nocivas.	Intermediário
Configuração de cofre de senhas para armazenamento decredenciais, chaves e outros dados sensíveis.	Intermediário
Automação do provisionamento e gerência de configuração de serviços e recursos de nuvem com modelo de infraestrutura como código e autosserviço.	Alta
Implementação de solução para gerenciamento e automaçãode backup de dados nos serviços de nuvem ou ambiente on-premises.	Intermediário
Implementação de solução para backup de dados de longaretenção com políticas de ciclo de vida.	Intermediário

Implementação de processos de transferência de grandes volumes de dados para nuvem, incluindo processo de backup e restauração em novo ambiente.	Intermediário
Desenho e implantação de arquitetura para continuidade de negócios e recuperação de desastres em ambiente de nuvemde acordo com requisitos de RTO (Recovery Time Objective) e RPO (Recovery Point Objective).	Especialista
Apresentação de workshops/transferência de conhecimentopara detalhamento de entregáveis.	Baixa
Configuração de estrutura de contas em conformidade commelhores práticas de segurança.	Intermediário
Avaliação de ambiente em nuvem sobre perspectiva de segurança, desempenho, confiabilidade, custos e eficiência operacional e aplicação de correções apropriadas.	Alta
Migração fim-a-fim de máquinas virtuais incluindo os processos de conversão, importação, configuração e testes do ambiente migrado.	Alta
Implementação de ambiente para virtualização de desktops, incluindo configuração de redes, autenticação, políticas de gerenciamento e imagens personalizadas com configurações e aplicativos.	Alta
Gerenciamento dos provedores de serviço, orquestração, bilhetagem, implementação de mecanismos de controle, otimização de custos, sustentação e operação de ambiente de Nuvem com execução de tarefas do dia a dia: monitoramento, aplicações de patches, backup, atendimento de requisições de tarefas e mudanças.	Baixa
Serviço de monitoramento dos recursos e componentes dasolução.	Baixo
Desenvolvimento de Contratos Inteligentes (Smart Contracts): Criação de programas autônomos que executam automaticamente acordos digitais baseados em condições predefinidas.	Alta
Implementação de Lógica de Negócios em Contratos Inteligentes: Definição e codificação das regras e operações que regem a execução dos contratos inteligentes.	Alta
Desenvolvimento de Interfaces de Usuário para DApps (Aplicações Descentralizadas): Criação de interfaces gráficas para facilitar a interação dos usuários com aplicativos descentralizados.	Alta
Integração de Contratos Inteligentes com APIs Externas: Conexão e comunicação dos contratos inteligentes com fontes externas de dados e serviços através de APIs.	Alta
Desenvolvimento de Oráculos para Obter Dados Externos: Implementação de mecanismos que fornecem informações externas confiáveis para os contratos inteligentes.	Alta

Desenvolvimento de Tokens e Protocolos de Tokenização: Criação de tokens digitais e definição dos protocolos para emissão, transferência e gerenciamento desses ativos na blockchain.	Alta

Desenvolvimento de Sistemas de Governança Descentralizada (DAOs): Construção de estruturas organizacionais autônomas que permitem aos participantes tomarem decisões coletivas na rede blockchain.	Alta
Desenvolvimento de Soluções de Escalonamento e Camadas de Segurança: Implementação de tecnologias para aumentar a capacidade de processamento e melhorar a segurança da rede blockchain.	Alta
Implementação de Soluções de Identidade Digital e Autenticação: Desenvolvimento de mecanismos para verificar e autenticar identidades digitais na blockchain.	Alta
Desenvolvimento de Wallets Criptográficas e Gerenciamento de Chaves: Criação de carteiras digitais seguras para armazenar chaves privadas e gerenciar transações na blockchain.	Alta
Implementação de Mecanismos de Privacidade e Segurança: Integração de técnicas e protocolos para proteger a privacidade dos dados e garantir a segurança das transações na blockchain.	Alta
Desenvolvimento de Soluções de Interoperabilidade entre Blockchains: Criação de pontes e protocolos para permitir a comunicação e transferência de dados entre diferentes blockchains.	Alta
Implementação de Mecanismos de Pagamento e Transações Off-Chain: Desenvolvimento de soluções para facilitar pagamentos e transações fora da cadeia principal da blockchain.	Alta
Desenvolvimento de Aplicações DeFi: Construção de aplicativos para oferecer serviços financeiros descentralizados, como empréstimos, staking e trocas de ativos.	Alta
Desenvolvimento de Soluções de NFT: Criação de padrões e plataformas para tokenização de ativos digitais não fungíveis na blockchain.	Alta
Testes de Desempenho e Escalabilidade da Rede Blockchain: Avaliação e otimização do desempenho e da capacidade de escala da infraestrutura blockchain.	Alta
Desenvolvimento de APIs para Integração com Outras Plataformas: Criação de interfaces de programação para permitir a integração de sistemas externos com a blockchain.	Alta

ANEXO F - LISTA DE PERFIS TÉCNICOS

1. A tabela a seguir estabelece relação entre os perfis técnicos dos recursos a serem alocados na execução dos serviços, sejam profissionais ou materiais, com o peso adotado do para efeito de cálculo do esforço considerado no dimensionamento de USTs do serviço.

Item	Perfil Técnico	Requisitos Técnicos Mínimos Obrigatórios de Enquadramento	Peso
1	Auxiliar Técnico I	**Do Auxiliar Técnico de TIC de Nível I** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência comprovada e no mínimo 01 (um) ano em atividades e funções correlatas ao serviço. **Do Auxiliar Técnico de Processo de Negócio de Nível I** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com o processo de negócio objeto da atividade, com experiência comprovada e no mínimo 01 (um) ano em atividades e funções correlatas ao serviço.	0,25
2	Auxiliar Técnico II	**Do Auxiliar Técnico de TIC de Nível II** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência comprovada e no mínimo 02 (dois) anos em atividades e funções correlatas ao serviço. **Do Auxiliar Técnico de Processo de Negócio Nível II** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com o processo de negócio objeto da atividade, com experiência comprovada e no mínimo 02 (dois) anos em atividades e funções correlatas ao serviço.	0,50
3	Técnico I	**Do Técnico de TIC de Nível I** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 03 (três) anos em atividades e funções correlatas ao serviço. **Do Técnico de Processo de Negócio Nível I** Enquadram-se profissionais com formação de nível médio em qualquer área compatível área compatível com o processo de negócio objeto da atividade, com experiência mínima de, 03 (três) anos em atividades e funções correlatas ao serviço.	1
4	Técnico II	**Do Técnico de TIC de Nível II** Enquadram-se profissionais com formação de nível superior em andamento com, pelo menos, 50% (cinquenta por cento) do curso concluído em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço com experiência comprovada de no mínimo 03 (três) anos em atividades e funções correlatas ao serviço. Ou Alternativamente, profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 05 (cinco) anos em atividades e funções correlatas ao serviço. **Do Técnico de Processo de Negócio Nível II** Enquadram-se profissionais com formação de nível superior em andamento	1,5

		com, pelo menos, 50% (cinquenta por cento) do curso concluído em área compatível	

		com o processo de negócio objeto da atividade, com experiência comprovada de no mínimo 03 (três) anos em atividades e funções correlatas ao serviço. Ou Alternativamente, profissionais com formação de nível médio em qualquer em área compatível com o processo de negócio objeto da atividade, com experiência comprovada mínima de 05 (cinco) anos em atividades e funções correlatas ao serviço.	
5	Analista I	**Do Analista de TIC de Nível I** Enquadram-se os profissionais com formação de nível superior em área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 05 (cinco) anos em atividades e funções correlatas ao serviço, **Do Analista de Processo de Negócio Nível I** Enquadram-se profissionais com formação de nível superior compatível com o processo de negócio objeto da atividade, com experiência mínima de 05 (cinco) anos em atividades e funções correlatas ao processo objeto da atividade.	2,0
6	Analista II	**Do Analista de TIC de Nível II** Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Lato Sensu) concluída ou em andamento em área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 06 (seis) anos em atividades e funções correlatas ao serviço; Ou, Alternativamente, formação de nível superior compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 08 (oito) anos em atividades e funções correlatas ao serviço. **Do Analista de Processo de Negócio Nível II** Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Lato Sensu) concluída ou em andamento em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de no mínimo 06 (seis) anos em atividades e funções correlatas ao processo objeto da atividade. Ou, Alternativamente, formação de nível superior compatível com o processo de negócio objeto da atividade, com experiência mínima de 08 (oito) anos em atividades e funções correlatas ao processo objeto da atividade.	2,50

7	Especialista I	**Do Especialista de TIC de Nível I** Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Lato Sensu) compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 07 (sete) anos em atividades e funções correlatas ao serviço; Ou, Alternativamente, formação de nível superior compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao serviço. **Do Especialista de Processo de Negócio Nível I** Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Lato Sensu) em área compatível com o processo de negócio objeto da	3,00

		atividade, com experiência comprovada de, no mínimo, 07 (sete) anos em atividades e funções correlatas ao processo objeto da atividade. Ou, Alternativamente, formação de nível superior compatível com o processo de negócio objeto da atividade, com certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao processo objeto da atividade.	
8	Especialista II	**Do Especialista de TIC de nível II** Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Stricto Sensu) compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço e experiência comprovada de, no mínimo, 08 (oito) anos em atividades e funções correlatas ao serviço, Ou, Alternativamente, formação de nível superior e pós-graduação (no mínimo Lato Sensu) compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao serviço. **Do Especialista de Processo de Negócio nível II** Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Stricto Sensu) em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de, no mínimo, 08 (oito) anos em atividades e funções correlatas ao processo objeto da atividade; Ou, Alternativamente, formação de nível superior e pós-graduação (no mínimo Lato Sensu) compatível com o processo de negócio objeto da atividade, com certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao processo objeto da atividade.	3,50

2. Com vistas a favorecer o processo de precificação do serviço no que se refere a alocação de recursos necessários ao serviço, considerada a necessidade de execução contínua de dadas atividades, a aceitabilidade definida dos perfis por serviços relacionados no catálogo de serviços, e cenários atuais relativos aos serviços demandados, estima-se que para correta execução dos serviços, os recursos necessários serão alocados com base na seguinte distribuição de tempo:

Perfil Técnico	**Alocação estimada**
Auxiliar I	17%
Auxiliar II	17%
Técnico I	16%
Técnico II	16%
Analista I	16%
Analista II	8%

Especialista I	5%
Especialista II	5%

3. Considerando os serviços listados no catálogo, seus pesos e distribuições adote-se apenas como referência para precificação, o fator médio de 1,368 para conversão entre horas de alocação e UST conforme a seguinte fórmula: Número de horas alocadas = (Número de UST_mês/(1,368*COMPLEXIDADE)). Esse fator foi definido com consideração a média de todos os pesos aplicáveis aos serviços no catálogo, permitindo uma aproximação do quantitativo em horas, da alocação necessária de recursos para a execução dos serviços.
   3.1. A CONTRATADA deverá propor um fator diferente do fator médio para aqueles casos em que a alocação real não está de acordo com a alocação estimada, o qual será avaliado pela CONTRATANTE.

ANEXO G - DO ACORDO DE NÍVEIS DE SERVIÇOS – SLA

1. A gestão e fiscalização do contrato se darão mediante o estabelecimento e acompanhamento de indicadores de desempenho, disponibilidade e qualidade, que comporão o Acordo de Nível de Serviço (SLA) entre a Contratante e Contratada.
2. Será de responsabilidade da CONTRATANTE o atendimento de 1º nível.
3. A manutenção corretiva consistirá no conserto de defeitos e/ou falhas de funcionamento apresentados nos sistemas implementados na nuvem e deverão ser realizados em 2º e 3º níveis de segunda a sexta-feira, exceto feriados, no horário de 8:00 às 18:00 horas, a critério da administração.
   3.1. Os chamados de 2º e 3º níveis fora destes períodos (emergenciais) deverão ser atendidos pelo serviço de plantão, independentemente de ser sábado, domingo ou feriado. Os chamados de plantão incorrem em uma remuneração adicional medida em Unidades de Suporte Técnico (UST).
4. Os incidentes, situações inesperadas e não programadas, deverão ser atendidas pelos serviços de suporte da CONTRATADA. Os incidentes têm a seguinte classificação:

   Severidade 1 ou Alta: Ambiente/Sistema está indisponível ou usuário sem acesso;

   Severidade 2 ou Média: Uma função do Ambiente/Sistema está indisponível;

   Severidade 3 ou Baixa: O Ambiente/Sistema está disponível, porém apresentando lentidão, erros que forçam o reinício do sistema e/ou de operações no mesmo, e/ou alguma intermitência em seu funcionamento.

   4.1. A CONTRATADA deverá prestar, durante a vigência deste contrato, serviços de suporte a produção e manutenção corretiva abrangendo no mínimo:
   4.2. Investigação e resolução de problemas no ambiente, mesmo que para isso seja necessário acionar o suporte do fabricante;
   4.3. Nível de serviço (SLA), para chamados abertos entre o horário compreendido entre as 08 horas e 18 horas, em dias úteis, conforme tabela a seguir:

Severidade	Descrição	Prazo máximo para início do atendimento remoto	Prazo máximo para a solução remota	Prazo máximo para início do Atendimento Presencial	Prazo máximo de Solução
1 - Crítica	Situação emergencial ou problema crítico que cause a indisponibilidade de sistema.	Até 2 horas	Até 8 horas	Até 12 horas após abertura do chamado remoto	Até 24 horas após abertura do chamado remoto
2 - Alta	Impacto de alta significância relacionado à utilização da solução: ocorrência de indisponibilidade de funcionalidade.	Até 4 horas	Até 16 horas	Até 48 horas após abertura do chamado remoto	Até 72 horas após abertura do chamado remoto

3 - Média	Impacto de baixa Significância relacionado à utilização da solução. Não há ocorrência de indisponibilidade de funcionalidade, sendo contornável por solução paliativa sem grandes esforços ou retrabalho.	Até 6 horas	Até 24 horas	Até 72 horas após abertura do chamado remoto	Até 96 horas após abertura do chamado remoto

4.4. Caso seja necessário o complemento de informações para atendimento do chamado, que impossibilitem a resolução do chamado pela CONTRATADA, a CONTRATANTE será solicitada para fornecer a informação e os prazos serão suspensos ou prorrogados até o recebimento das informações.
4.5. O tempo em horas, previsto no SLA, será computado a partir da abertura do chamado até a sua regularização, nesse caso, uma solução de contorno poderá ser utilizada, caso a solução definitiva não seja possível de ser executada imediatamente.
4.6. A CONTRATADA deverá atender no mínimo 90% (noventa por cento) dos chamados dentro do SLA estabelecido na tabela.

ANEXO H - Modelo de Proposta

Tabela 1 – Plataforma em nuvem de Solução de visibilidade e detecção de ameaças do tráfego de rede e SSL Decryption Universal.

ITEM	DESCRIÇÃO	UNIDADE	QTDE (A)	VALOR UNITÁRIO (B)	VALOR TOTAL (C = A X B x 12)
1	Serviço de Interceptação do Tráfego – Tipo 1.	Serviço	6,0		
2	Serviço de Interceptação do Tráfego – Tipo 2.	Serviço	4,0		
3	Serviço de Interceptação do Tráfego - Tipo 3.	Serviço	2,0		
4	Serviço de Descriptografia do Tráfego – Compatível com os Equipamentos do Tipo 1 e 2.	Serviço	10,0		
5	Serviço de Descriptografia do Tráfego – Compatível com o Equipamento do Tipo 3.	Serviço	2,0		
6	Serviço para o Tratamento do Tráfego de Aplicações – Compatível com os Equipamentos do Tipo 1 e 2.	Serviço	8,0		
7	Serviço para o Tratamento do Tráfego de Aplicações – Compatível com o Equipamento do Tipo 3.	Serviço	4,0		
8	Gerenciamento Centralizado da Solução.	Serviço	12,0		
9	Serviço de Interceptação do Tráfego Virtualizado Essencial.	Serviço	4,0		
10	Serviço de Interceptação do Tráfego Virtualizado Avançado.	Serviço	4,0		
11	Serviço centralizado de Chassi para Interconector Passivo de Interceptação do Tráfego - Interfaces Ópticas	Serviço	12,0		
12	Serviço de Interconector Passivo de Interceptação do Tráfego – Interfaces SFP	Serviço	40,0		

13	Serviço de Interconector Passivo de Interceptação do Tráfego – Interfaces QSFP	Serviço	40,0		
14	Serviço de Interconector Passivo de Interceptação do Tráfego – Interfaces RJ-45	Serviço	40,0		
15	Serviço de Concentrador de Tráfego de Segurança.	Serviço	12,0		
16	Serviço de Transceivers Tipo 1 – 1 Gbps Ethernet	Serviço	40,0		
17	Serviço de Transceivers Tipo 2 – 10 Gbps Ethernet	Serviço	40,0		
18	Serviço de Transceivers Tipo 3 – 25 Gbps Ethernet	Serviço	40,0		
19	Serviço de Transceivers Tipo 4 – 40 Gbps Ethernet	Serviço	40,0		
20	Serviços de Transceivers Tipo 5 – 100 Gbps Ethernet	Serviço	40,0		
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QTDE (A)**	**VALOR UNITÁRIO (B)**	**VALOR TOTAL (C = A X B)**
21	Serviços de Operação Assistida e ajuste fino para as Soluções de NPB	UST	40.000		
Valor Total Soma (D)				R$	

(T1) Valor Total em R$ (igual a "D")

_____

Valor Total da Proposta (T1)

_____