PREGÃO ELETRÔNICO Nº 043/2024

EXPEDIENTE Nº 0429/24

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM SERVIÇOS DE MONITORAMENTO E GERENCIAMENTO DE TRÁFEGO DA REDE DE DADOS DA COMPANHIA DE ENGENHARIA DE TRÁFEGO CET, COM MANUTENÇÃO E SUPORTE, POR UM PERÍODO DE 24 (VINTE E QUATRO) MESES.

CONTRATO Nº 002/2025

ÍNDICE

Cláusula Primeira - Do Objeto Contratual

Cláusula Segunda - Da Vigência e Prazos

Cláusula Terceira - Das Condições de Prestação dos Serviços

Cláusula Quarta - Das Obrigações e Responsabilidades da Contratada

Cláusula Quinta - Das Obrigações da CET

Cláusula Sexta – Da Fiscalização dos Serviços

Cláusula Sétima - Do Valor e Preços

Cláusula Oitava - Da Medição/Forma de Pagamento

Cláusula Nona - Do Reajuste

Cláusula Décima - Dos Impostos e Incidências Fiscais

Cláusula Décima Primeira - Das Garantias

Cláusula Décima Segunda - Das Penalidades

Cláusula Décima Terceira - Da Subcontratação

Cláusula Décima Quarta - Da Rescisão

Cláusula Décima Quinta - Do Recebimento do Objeto

Cláusula Décima Sexta – Da Possibilidade de Alteração

Cláusula Décima Sétima - Da Legislação Aplicável

Cláusula Décima Oitava – Da Proteção de Dados Pessoais

Cláusula Décima Nona - Das Disposições Finais e Confidencialidade

Cláusula Vigésima - Do Foro

EXPEDIENTE Nº 0429/24

CONTRATO Nº 002/2025, CELEBRADO ENTRE A COMPANHIA DE ENGENHARIA DE TRÁFEGO - CET E NUNTIUS CONSULTORIA E ENGENHARIA LTDA

A **COMPANHIA DE ENGENHARIA DE TRÁFEGO - CET**, com sede nesta Capital na Rua Barão de Itapetininga nº 18, inscrita no CNPJ sob o nº 47.902.648/0001-17, neste ato representada por seus Representantes Legais ao final assinados, doravante designada **CET** e a empresa **NUNTIUS CONSULTORIA E ENGENHARIA LTDA** com sede nesta Capital, na Rua Mairinque, nº 61, conj. 508, Vila Clementino, CEP 04037-020, com Telefone(s) nº(s) 11 4210-0562, inscrita no CNPJ sob o nº 16.657.548/0001-49 e Inscrição Estadual nº 142.413.660.112, neste ato representada por seu(s) Representante(s) Legal(is) ao final assinado(s), doravante designada **CONTRATADA**, têm entre si justo e contratado o seguinte:

CLÁUSULA PRIMEIRA - DO OBJETO CONTRATUAL

1.1. Constitui objeto deste Contrato, pelo regime de empreitada por preço unitário, a prestação de serviços de monitoramento e gerenciamento de tráfego da Rede da Companhia de Engenharia de Tráfego – CET, com manutenção e suporte técnico nas seguintes unidades localizadas no município de São Paulo: Rua Bela Cintra, nº 385, Consolação e Rua Sumidouro nº 740, Pinheiros, obrigando-se a **CONTRATADA** a executá-lo de acordo com o **PREGÃO ELETRÔNICO Nº 043/24,** com o ***Anexo I - Termo de Referência***, com o ***Anexo II - Proposta*** e demais elementos que compõem o expediente mencionado no preâmbulo, os quais passam a integrar este instrumento.

CLÁUSULA SEGUNDA - DA VIGÊNCIA E PRAZOS

2.1. O prazo total do presente Contrato é de 24 (vinte e quatro) meses, contados a partir data da sua assinatura, podendo ser prorrogado sucessivamente, em prazo inferior, igual ou superior ao contrato inicial, até o limite legal.

2.2. Os prazos para a execução dos serviços estão previstos no **Anexo I - Termo de Referência**.

CLÁUSULA TERCEIRA - DAS CONDIÇÕES DE PRESTAÇÃO DOS SERVIÇOS

3.1. As condições de prestação dos serviços estão dispostas no **Anexo I - Termo de Referência.**

CLÁUSULA QUARTA - DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

4.1. Atender a todas as exigências deste Contrato e do **Anexo I- Termo de Referência** do Edital.

4.2. A **CONTRATADA** se obriga a selecionar, designar e manter profissionais cuja qualificação esteja em conformidade com os tipos de serviços contratados observando as linguagens, ferramentas ou tecnologias a serem implementadas com o acompanhamento desta**.**

4.3. Fornecer a infraestrutura de plataforma de virtualização necessária para funcionamento da solução de detecção de ameaças rede.

4.4. A plataforma de virtualização da **CONTRATADA** deverá permitir rodar máquinas virtuais (VMs) compatíveis com os sistemas operacionais baseados em Linux de 64 bits ou Windows Server 2022 (ou superior).

4.5. As máquinas virtuais (VMs) da solução de detecção de ameaças de rede serão instalados em duas localidades diferentes, sendo uma (1) VM no site Bela Cintra e uma (1) VM no site Sumidouro**.**

4.6. A **CONTRATADA** deverá garantir que todos os equipamentos, softwares, componentes, acessórios e cabos de conexão para interligar fisicamente a solução sejam entregues**.**

4.7. A **CONTRATADA** deverá assegurar a instalação de todos os softwares e ferramentas que acompanham a solução ofertada, de acordo com o detalhamento constante **no item 6** do **Anexo I – Termo de Referência.**

4.8. A **CONTRATADA** deverá fornecer instalação, customização, montagem física dos equipamentos e seus respectivos acessórios, além de toda configuração lógica, para todos os produtos (hardware e software), de acordo com as especificações constantes no **Anexo I – termo de Referência.**

4.9. Correrão por conta da **CONTRATADA** as despesas com o frete, transporte, seguro e demais custos advindos da entrega dos produtos.

4.10. A **CONTRATADA** deverá entregar qualquer componente da solução, a partir da assinatura do contrato, em até 60 (sessenta) dias corridos. Atrasos na entrega serão aceitos mediante condições extraordinárias e deverão ser avisados com antecedência máxima de até 15 (quinze) dias corridos prévios ao limite do prazo.

4.11. A **CONTRATADA** deverá realizar treinamento e capacitação na solução ofertada para 02 (duas) turmas de 05 (cinco) colaboradores da **CET**, com carga horária mínima de 32 (trinta e duas) horas cada turma e com o conteúdo necessário para que as equipes da **CET** sejam capacitadas a administrar a solução ofertada, bem como, realizar customizações em suas configurações e instalar novos *scanners/agentes* e realizar integrações com ferramentas de terceiros, de acordo com o detalhamento constante **no item 7** do **Anexo I – Termo de Referência.**

4.12. A **CONTRATADA** deverá fornecer suporte técnico prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, de acordo com o detalhamento constante **no item 8** do **Anexo I – Termo de Referência.**

4.13. A **CONTRATADA** se obriga a selecionar, designar e manter profissionais cuja qualificação esteja em conformidade com os tipos de serviços contratados observando as linguagens, ferramentas ou tecnologias a serem implementadas com o acompanhamento desta.

4.14. Responsabilizar-se por todas as despesas com material, mão-de-obra, acidentes de trabalho, encargos trabalhistas, previdenciários, fiscais e comerciais, transportes, seguros operacionais, taxas, tributos, contribuições de qualquer natureza ou espécie e quaisquer outras

despesas necessárias à perfeita execução dos serviços contratados.

4.15. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

4.16. Responsabilizar-se pelos danos causados diretamente à **CET** ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato, não excluindo ou reduzindo essa responsabilidade à fiscalização ou ao acompanhamento da **CET.**

4.17. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

4.18. A **CONTRATADA** obrigar-se-á a entregar os serviços estritamente de acordo com as especificações constantes do **Anexo I - Termo de Referência**, responsabilizando-se pelo refazimento total ou parcial, na hipótese de se constatar defeitos na execução ou estiver em desacordo com as especificações adotadas.

4.19. Manter-se durante toda a execução do objeto do contrato em compatibilidade com as obrigações por ela assumidas e todas as condições de habilitação e qualificação exigidas na licitação.

CLÁUSULA QUINTA - DAS OBRIGAÇÕES DA CET

5.1. Designar o Gestor e o fiscal do Contrato para acompanhamento e fiscalização do Contrato.

5.2. Exercer o acompanhamento e fiscalização dos serviços, através de empregados designados, verificando se o objeto está sendo executado, sendo que esse acompanhamento não isenta a efetiva **CONTRATADA** da necessidade de realizar a supervisão dos serviços.

5.3. Esclarecer prontamente as dúvidas que lhe sejam apresentadas pela **CONTRATADA**.

5.4. Comunicar, imediatamente à **CONTRATADA** as possíveis irregularidades detectadas quando da execução dos serviços, formulando exigências necessárias às respectivas regularizações.

5.5. Proporcionar as condições para que a **CONTRATADA** possa desempenhar seus serviços de acordo com as determinações do Edital e desse Contrato.

5.6. O fornecimento da infraestrutura de servidores necessários para funcionamento da solução de detecção de ameaças rede será de responsabilidade da **CET.**

5.7. A **CET** fornecerá infraestrutura para rodar até duas (2) VMs de acordo com os requisitos de hardware especificados no subitem 5.2 do **Anexo I – Termo de Referência**.

5.8. Os chamados para o suporte técnico serão feitos pela **CET** e classificados por grau de severidade, de acordo com o impacto no ambiente da **CET**, sendo que o nível de severidade será atribuído pela **CET** no momento da abertura do chamado.

5.9. A **CET** deverá prestar as informações e os esclarecimentos que porventura venham a ser solicitados pela **CONTRATADA**.

5.10. A **CET** deverá permitir, durante a vigência do contrato, o acesso dos representantes ou prepostos da **CONTRATADA** às suas dependências, desde que devidamente identificados e

acompanhados por representante da **CET.**

5.11. A **CET** deverá promover o acompanhamento e a fiscalização desta contratação, sob os aspectos quantitativo e qualitativo, anotando em registro próprio as falhas detectadas, comunicando as ocorrências de quaisquer fatos que exijam medidas corretivas por parte da **CONTRATADA.**

5.12. A **CET**, após as devidas notificações formalizadas e não atendidas, reserva para si o direito de aplicar sanções ou rescindir o contrato, após o decurso do prazo estabelecido não atendido, no caso de inobservância pela **CONTRATADA** de quaisquer condições estabelecidas no **Anexo I - Termo de Referência**, em especial após a constatação do inadimplemento.

5.13. Rejeitar os serviços realizados fora do estabelecido e que estejam em desacordo com as especificações.

5.14. Efetuar o pagamento à **CONTRATADA** de acordo com as condições de preço e prazo estabelecidas nesse contrato.

5.15. Atestar a execução do objeto por meio do Gestor designado.

CLÁUSULA SEXTA - DA FISCALIZAÇÃO DOS SERVIÇOS

6.1. Não obstante a **CONTRATADA** seja a única e exclusiva responsável pelos serviços do objeto deste contrato, a **CET**, sem restringir a plenitude dessa responsabilidade, exercerá o direito de fiscalizar o fiel cumprimento das especificações exigidas, a fim de assegurar o seu recebimento ou manifestar sua recusa.

6.2. A fiscalização será exercida consoante o disposto no Capítulo X do Regulamento Interno de Licitações, Contratos e Convênios – RILCC da **CET** e no interesse exclusivo da **CET** e não implica em sua corresponsabilidade, não excluindo nem reduzindo a responsabilidade da **CONTRATADA**, inclusive por danos que possam ser causados a **CET** ou a terceiros, por qualquer irregularidade decorrente de culpa ou dolo da **CONTRATADA** na execução dos serviços.

6.3. No curso da execução dos serviços e em sua entrega, a **CET** fiscalizará o cumprimento da execução do objeto, conforme as especificações exigidas, com vistas ao recebimento a contento do objeto.

6.4. A **CET** registrará as deficiencias porventura existentes na execução dos serviços e/ou inobservâncias dos aspectos de segurança envolvidos, comunicando-as à **CONTRATADA** para imediata correção, sem prejuízo da aplicação das penalidades previstas.

6.5. A **CET** poderá embargar, a qualquer tempo a execução de serviços que não estejam sendo cumpridos de acordo com as disposições destas condições e/ou com a boa técnica ou que atente contra a segurança e bens da **CET** e/ou serviços, bem como recusar os já executados.

6.6. A **CET** aplicará penalidade, de acordo com o disposto na Cláusula Penalidades quando for constatada qualquer irregularidade/descumprimento das obrigações contratuais.

6.7. A fiscalização não exclui nem reduz a responsabilidade da **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, e na ocorrência desta, não implicará em corresponsabilidade da **CET** e/ou de seus agentes ou prepostos.

CLÁUSULA SÉTIMA - DO VALOR E PREÇOS

7.1. O valor total do presente Contrato, para 24 (vinte e quatro) meses, é de **R$ 9.728.931,00 (nove milhões, setecentos e vinte e oito mil, novecentos e trinta e um reais),** em função dos preços indicados na Proposta, na data base de **19/12/2024.**

7.2. Os preços unitários objeto deste são:

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR (R$)	
			Preço Unitário	Preço Total
7.2.1.1	Máquina física (equipamentos agregadores de tráfego).	02	359.023,47	718.046,94
7.2.1.2	Dispositivos utilizados para monitorar e capturar o tráfego de rede de dados – TAPs (Test Access Points) no padrão 1/10G LX/LR **monomodo** para fibras com conector LC.	24	17.464,17	419.140,08
7.2.1.3	Dispositivos utilizados para monitorar e capturar o tráfego de rede de dados – TAPs (Test Access Points) no padrão 1/10G SX/SR **multimodo** para fibras com conector LC.	24	16.526,83	396.643,92
7.2.1.4	Transceivers de 1Gb Base1000T.	16	5.410,85	86.573,60
7.2.1.5	Transceivers de 1Gb Base SX.	16	5.809,07	92.945,12
7.2.1.6	Transceivers de 1Gb Base LX.	16	7.493,52	119.896,32
7.2.1.7	Licenças de software da solução de gerenciamento centralizada dos Network Packet Brokers e agregadores de tráfego dos TAPs.	02	1.298.831,57	2.597.663,14
7.2.2	Solução de Observabilidade de Rede	01	2.136.854,77	2.136.854,77
7.2.3	Detecção e Resposta à Ameaças em Rede	01	2.168.305,64	2.168.305,64
7.2.4	Treinamento	02	43.468,33	86.936,66
7.2.5	Suporte técnico prestados em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, por 24 meses.	01	905.924,81	905.924,81
PREÇO TOTAL PARA 24 MESES				**9.728.931,00**

7.3. O preço total para a execução dos serviços, é o constante da proposta comercial da licitante e remunerará todas as despesas necessárias à execução dos serviços ora contratados e todos os custos básicos diretos, bem como o frete, transporte, encargos sociais e trabalhistas, previdenciários, fiscais ou quaisquer outros que incidam ou venham a incidir direta ou indiretamente sobre o objeto deste Contrato.

CLÁUSULA OITAVA - DA MEDIÇÃO/FORMA DE PAGAMENTO

8.1. A medição dos serviços executados será realizada mensalmente a contar da data de assinatura do contrato, pela fiscalização da **CET** e em conformidade com as condições estabelecidas no **Anexo I - Termo de Referência e com os valores contratuais**.

8.1.1. O pagamento dos ***itens 7.2.1.1 a 7.2.1.7, 7.2.2 e 7.2.3*** serão efetuados em parcela única,

após a instalação dos equipamentos e do ***item 7.2.4*** será efetuado após realização do treinamento para as 02 (duas) turmas previstas.

8.1.2. O pagamento do ***item 7.2.5***, será efetuado em uma única vez, porém para Suporte Técnico prestado em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, por 24 meses de acordo com as condições estabelecidas no **item 8** do **Anexo I – Termo de Referência** e neste Contrato.

8.2. O período de apuração das medições será do dia 11 (onze) de cada mês ao dia 10 (dez) do mês subsequente.

8.3. A **CET** confirmará se todos os serviços prestados no período, ou seja, do dia 11 (onze) de cada mês ao dia 10 (dez) do mês subsequente, serão considerados como válidos.

8.4. Com base na medição aprovada pela **CET**, a **CONTRATADA** emitirá Nota Fiscal Eletrônica ou documento equivalente, correspondente aos serviços prestados, que será paga, no prazo de 30 (trinta) dias corridos, contados a partir do adimplemento da obrigação, onde constarão as quantidades medidas e aprovadas, multiplicadas pelos preços unitários constantes deste Contrato.

8.5. Além da Nota Fiscal Eletrônica ou documento equivalente, o pedido de pagamento deverá ser acompanhado da prova de inexistência de registro no CADIN do Município de São Paulo e das Certidões de regularidade fiscal/trabalhista em vigência.

8.5.1. Caso a **CONTRATADA** durante a vigência do Contrato não cumprir com o exigido na **cláusula 4.19** ou vier a ser inscrita no CADIN MUNICIPAL, deverá fazer prova de regularização das Certidões e de débito(s) inscrito(s), ficando sujeita à suspensão do pagamento do serviço enquanto não ficar comprovada a sua regularidade junto ao respectivo cadastro e da documentação.

8.6. Ocorrendo eventual atraso no pagamento, o valor do principal devido será reajustado utilizando-se o índice oficial de remuneração básica da caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança para fins de compensação da mora (TR + 0,5% "pro-rata tempore"), observando-se, para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorreu, nos termos da Portaria 5/12 da Secretaria das Finanças.

8.7. O pagamento será efetuado exclusivamente em conta corrente bancária a ser indicada pela **CONTRATADA.** A informação deverá ser encaminhada para a Gerência Financeira - GFI na Rua Barão de Itapetininga nº 18 - 4º andar - Centro/SP.

8.8. Caso a **CONTRATADA** solicite que o pagamento seja creditado em conta corrente de outro banco que não o indicado, arcará com todas as despesas e tarifas bancárias vigentes, incorridas na transação de pagamento: DOC, TED, tarifa de emissão de cheque e outras.

8.9. A **CONTRATADA** deverá encaminhar os arquivos eletrônicos para a Gerência Financeira - GFI (e.mail: gfi@cetsp.com.br) no caso de utilização da DANFE, ficando o pagamento condicionado ao encaminhamento desses arquivos.

8.10. Caso o documento fiscal seja apresentado com erro, será devolvido para correção, contando-se novo prazo para análise, aprovação e pagamento a partir da reapresentação.

8.11. Nenhum pagamento isentará a **CONTRATADA** das responsabilidades contratuais, nem implicará na aceitação do fornecimento/instalação pela **CET**.

CLÁUSULA NONA - DO REAJUSTE

9.1. Os preços contratados somente poderão ser reajustados após um ano da data limite para

apresentação da proposta, pela variação do índice IPC-FIPE, com base na Portaria SF nº 389 de 18 de dezembro de 2017, que dispõe instruções para cumprimento excepcional do artigo 7º do Decreto Municipal nº 57.580/17 observando-se as demais normas que regulamentam a matéria.

9.2. As condições de reajustamento ora pactuadas poderão ser alteradas em face da superveniência de normas federais ou municipais aplicáveis à espécie.

CLÁUSULA DÉCIMA - DOS IMPOSTOS E INCIDÊNCIAS FISCAIS

10.1. Os tributos, taxas, impostos, emolumentos, contribuições previdenciárias, trabalhistas, fiscais e parafiscais que sejam devidos em decorrência, direta ou indireta, deste Contrato, serão de exclusiva responsabilidade da **CONTRATADA**, assim definido na legislação vigente, sem direito a reembolso.

CLÁUSULA DÉCIMA PRIMEIRA - DAS GARANTIAS

11.1. A **CONTRATADA** deverá apresentar à **CET** a Garantia de Execução Contratual, correspondente a 5% (cinco por cento) do valor total do presente Contrato, no prazo de até 10 (dez) dias úteis após a celebração do respectivo instrumento, sob pena de aplicação de multa, a fim de assegurar a sua execução e será prestada em qualquer das modalidades admitidas pelo § 1º do artigo 70 da Lei Federal nº 13.303/16 e § 1º do artigo 141 Regulamento Interno de Licitações, Contratos e Convênios - RILCC, regulamentada pela Portaria SF nº 76 de 22/03/2019 da Secretaria Municipal da Fazenda da Prefeitura do Município de São Paulo.

11.1.1. A multa referida na cláusula anterior correspondente a 0,1% (zero virgula um por cento) do valor total do Contrato, conforme inciso IV do artigo 193 do Regulamento Interno de Licitações, Contratos e Convênios – RILCC.

11.1.2. Em caso da **CONTRATADA** optar pela prestação da Garantia na modalidade de Fiança Bancária, deverá apresentar conforme o Anexo VIII - Modelo de Fiança Bancária, do Edital.

11.1.3. O prazo para a apresentação da garantia poderá ser prorrogado mediante solicitação e apresentação de justificativas a serem submetidas a apreciação pela CET.

11.2. A não apresentação da garantia, prevista na cláusula anterior, em até 20 (vinte) dias úteis, autorizará a rescisão unilateral do contrato por descumprimento ou cumprimento irregular de suas cláusulas, com a aplicação das penalidades de multa.

11.3. A garantia será devolvida à **CONTRATADA** em até 30 (trinta) dias da lavratura do Termo de Recebimento Definitivo do objeto e após a quitação das multas contratuais eventualmente existentes, atualizada monetariamente nos termos § 4º do artigo 141 do Regulamento Interno de Licitações, Contratos e Convênios – RILCC.

11.4. Se houver prorrogação ou acréscimo ao valor do Contrato, a **CONTRATADA** se obriga a fazer a complementação da garantia na assinatura do respectivo Termo Aditivo, ou excepcionalmente, no prazo máximo de 10 (dez) dias úteis, contados da data de assinatura do respectivo Termo Aditivo.

CLÁUSULA DÉCIMA SEGUNDA - DAS PENALIDADES

12.1. Pelo descumprimento das obrigações assumidas a **CONTRATADA** estará sujeita às penalidades de advertência e multas/sanções a seguir especificadas e cujo cálculo tomará por base o valor do Contrato nas mesmas bases do ajuste, com fundamento no Capítulo II, Seção III, art. 82 da Lei Federal nº 13.303/16 e Capítulo XIII do Regulamento Interno de Licitações, Contratos e Convênios – RILCC da **CET**, garantindo o contraditório e a ampla e prévia defesa:

12.1.1. ADVERTÊNCIA para os casos, a seguir especificados, de atrasos, descumprimento ou

apresentação de falhas nas obrigações contratuais e sempre que forem constatadas irregularidades de pouca gravidade e que o ato praticado pela **CONTRATADA**, ainda que ilícito, não seja suficiente para acarretar danos à **CET** e seus funcionários, suas instalações, imagem, meio ambiente ou a terceiros e que não justifique a imposição de sanção mais gravosa.

12.1.1.1. Não cumprimento do prazo estabelecido no ***subitem 6.11.1*** do **Anexo I - Termo de Referência,** para a realização de reunião de alinhamento on-site ou remoto, por responsabilidade da **CONTRATADA.**

12.1.1.2. Não cumprimento do prazo estabelecido no ***subitem 6.11.2*** do **Anexo I - Termo de Referência,** para a elaboração do plano de testes e validação, em conjunto com os técnicos da **CET**, após a instalação dos equipamentos constantes do objeto e/ou se os testes forem realizados comprometendo os ambientes de produção, durante o período de segunda a sexta-feira, das 07h00 às 19h00**.**

12.1.1.3. Não cumprimento do prazo estabelecido no ***subitem 6.11.3*** do **Anexo I - Termo de Referência,** para a entrega do material gerado em decorrência da reunião prevista no ***subitem 6.11.1.***

12.1.1.4. Não atendimento dos prazos para os chamados técnicos relacionados aos Níveis de Severidade 3 e 4 estabelecidos nos ***subitens 8.33.3 e 8.33.4*** do **Anexo I - Termo de Referência,** respectivamente.

12.1.2. Se, após a notificação de advertência pela **CET,** não ocorrer as entregas especificadas nos ***subitens 6.11.1 a 6.11.3, 8.33.3 e 8.33.4*** do **Anexo I - Termo de Referência,** será aplicada multa de 10% (dez por cento) do valor mensal do contrato.

12.1.3. Persistindo a situação descrita na ***Cláusula 12.1.2*** após a aplicação da multa, fica caracterizada Inexecução Parcial do Contrato, com aplicação da penalidade correspondente.

12.1.4. O não cumprimento do prazo de 60 (sessenta) dias corridos da assinatura do contrato, estabelecido ***no item 6.17*** do **Anexo I - Termo de Referência**, para a entrega dos componentes da solução, sem justificativas da **CONTRATADA** que caracterizem condições extraordinárias, acarretará multa de 10% dos valores correspondentes aos ***itens 7.2.1.1 a 7.2.1.7*** da ***Cláusula Sétima*** deste Contrato. Se, após a aplicação da penalidade não ocorrer a entrega, ficará caracterizada Inexecução Total do Contrato, com aplicação da penalidade correspondente.

12.1.5. O não atendimento do prazo para os chamados técnicos relacionados aos Níveis de Severidade 1 e 2 estabelecidos nos ***subitens 8.33.1 e 8.33.2*** do **Anexo I - Termo de Referência,** acarretará multa de 10% (dez por cento), por dia de atraso, sobre o valor mensal do contrato referente ao Suporte técnico ***(item 7.2.5*** da ***Cláusula Sétima*** deste Contrato)**,** até o limite máximo de 10 (dez) dias corridos, quando será caracterizada inexecução parcial do contrato, com aplicação da penalidade correspondente.

12.1.6. Multa de 5% (cinco por cento) sobre o valor contratual mensal, quando, sem justa causa aceita pela **CET,** a **CONTRATADA** não cumprir com qualquer outra obrigação assumida em decorrência do Contrato.

12.1.7.A pena de multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório e sua cobrança não isentará a **CONTRATADA** da obrigação de indenizar eventuais perdas e danos.

12.1.8. Pelo inadimplemento total ou parcial deste Contrato, independentemente da rescisão, a **CONTRATADA** ficará sujeita a critério da **CET** às seguintes penalidades:

12.1.8.1. Multa de 10% (dez por cento), por inexecução parcial do Contrato, mediante competente justificativa, **sobre o valor da parcela não executada**, nos termos do Art. 193, V do Regulamento Interno de Licitações, Contratos e Convênios - RILCC da CET.

12.1.8.2. Multa de 20% (vinte por cento), por inexecução total do Contrato, mediante competente justificativa, **sobre o valor total do Contrato**, nos termos do Art. 193, VI do Regulamento Interno de Licitações, Contratos e Convênios - RILCC da CET.

12.1.8.3. A inexecução parcial ou total do Contrato poderá ensejar sua rescisão nos termos do artigo nº 182 do Regulamento Interno de Licitações, Contratos e Convênios - RILCC da CET.

12.1.9. Suspensão temporária do direito de licitar e impedimento de contratar com a CET, por prazo não superior a 02 (dois) anos ou enquanto perdurarem os motivos determinantes da punição ou, ainda, até que seja promovida a reabilitação, quando houver, em especial:

a) reincidência de execução insatisfatória na prestação de serviços contratados;

b) atraso injustificado na execução/conclusão dos serviços, contrariando o disposto no contrato;

c) reincidência na aplicação das penalidades de multa;

d) irregularidades que ensejem a rescisão contratual;

e) condenação definitiva por praticar fraude fiscal no recolhimento de quaisquer tributos;

f) prática de atos ilícitos visando prejudicar a execução do contrato;

g) prática de atos ilícitos que demonstrem não possuir a Contratada idoneidade para contratar com a **CET**.

12.1.10. Declaração de inidoneidade para licitar e contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

a) A declaração de inidoneidade poderá ser proposta ao Diretor Presidente da **CET** quando constatada a má-fé, ação maliciosa e premeditada em prejuízo da **CET**, evidência de atuação com interesses escusos, inclusive apresentação de documentos falsos ou falsificados ou reincidência de faltas que acarretem prejuízos à **CET** ou aplicações sucessivas de outras penalidades.

12.1.11.A pena de multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório e sua cobrança não isentará a **CONTRATADA** da obrigação de indenizar eventuais perdas e danos.

12.1.12. Eventuais penalidades pecuniárias, aplicadas à **CONTRATADA** após o regular procedimento administrativo serão descontadas da garantia prestada pela **CONTRATADA.** Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a **CONTRATADA** pela sua diferença, a qual será descontada dos pagamentos vincendos que a **CONTRATADA** tenha a receber da **CET,** relativamente a este Contrato ou, ainda, ser cobrado administrativa ou judicialmente, conforme previsto no art. 82, §§ 2º e 3º da Lei Federal nº 13.303/2016.

12.1.13. Se o valor do pagamento for insuficiente, fica a **CONTRATADA** obrigada a recolher a importância devida no prazo de 15 (quinze) dias corridos, contado da comunicação oficial.

12.1.14. A compensação citada no item **12.1.12** ficará restrita ao âmbito do presente Contrato.

12.1.15. No caso de aplicação de eventuais penalidades, será observado o procedimento previsto no Regulamento Interno de Licitações, Contratos e Convênios – RILCC da **CET**.

12.1.16. Será remetida à Secretaria Municipal de Gestão - Seção de Cadastro de Fornecedores, cópia do ato que aplicar qualquer penalidade ou da decisão final do recurso interposto pela **CONTRATADA**, a fim de que seja averbada a penalização no cadastro municipal de fornecedores.

12.1.17. As sanções/multas são independentes e a aplicação de uma não exclui a das outras, sendo descontadas do pagamento respectivo ou, se for o caso, cobradas administrativa ou judicialmente.

CLÁUSULA DÉCIMA TERCEIRA - DA SUBCONTRATAÇÃO

13.1. Será permitida a subcontratação parcial do objeto, mediante consulta análise e aprovação da **CET**, sob pena de rescisão do Contrato e das sanções previstas na Lei Federal nº 13.303/16.

13.1.1. A empresa subcontratada deverá atender, em relação ao objeto da subcontratação, as exigências de **habilitação jurídica**, **regularidade fiscal e trabalhista** e de **qualificação técnica** aplicáveis à subcontratação, da forma como consta do Edital.

13.1.2. É vedada a subcontratação de empresa ou consórcio que tenha participado: I – do procedimento licitatório do qual se originou a contratação; II – direta ou indiretamente, da elaboração de projeto básico ou executivo.

13.2. A subcontratação restringe-se exclusivamente ao fornecimento de licenças de software e a compra de hardware de mercado.

13.3. O fornecimento poderá ser subcontratado somente após a autorização da **CET** e a **CONTRATADA** será responsável pelo mesmo.

13.3.1. A **CONTRATADA** será responsável pela supervisão, fiscalização e garantia da qualidade dos serviços executados pela(s) subcontratada(s).

13.3.2. Qualquer falha ou irregularidade na execução dos serviços subcontratados será imputada diretamente à **CONTRATADA,** a qual responderá integralmente perante a **CET.**

13.3.3. A **CONTRATADA** será solidariamente responsável por todos os atos, danos ou prejuízos causados pelas subcontratadas, incluindo a reparação de quaisquer danos materiais, morais ou patrimoniais, decorrentes da execução do objeto subcontratado.

CLÁUSULA DÉCIMA QUARTA - DA RESCISÃO

14.1. Constituem motivo para rescisão de contrato, dentre outros:

I - o não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;

II - a alteração da pessoa do contratado, mediante a subcontratação total ou parcial não autorizada pela CET do seu objeto , a associação do contratado com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não admitidas no edital ou no contrato;

III - o desatendimento das determinações regulares da **CET** decorrentes do acompanhamento e fiscalização do contrato;

IV - o cometimento reiterado de faltas na execução contratual;

V - a dissolução da sociedade ou o falecimento do contratado;

VI - a decretação de falência ou a insolvência civil do contratado;

VII - a alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique a execução do contrato;

VIII - razões de interesse da **CET**, de alta relevância e amplo conhecimento, justificadas e exaradas no processo administrativo;

IX - o atraso nos pagamentos devidos pela **CET** decorrentes de obras, serviços ou fornecimentos, ou parcelas destes, já recebidos ou executados, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado ao contratado o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;

X - a não liberação, por parte da **CET**, de área, local ou objeto para execução de obra, serviço ou fornecimento, nos prazos contratuais, bem como das fontes de materiais naturais especificadas no projeto;

XI - a ocorrência de caso fortuito, força maior ou fato do príncipe, regularmente comprovada, impeditiva da execução do contrato;

XII - a não integralização da garantia de execução contratual no prazo estipulado;

XIII - o descumprimento da proibição de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e de qualquer trabalho a menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos;

XIV - o perecimento do objeto contratual, tornando impossível o prosseguimento da execução da avença;

XV - ter frustrado ou fraudado, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público; ter impedido, perturbado ou fraudado a realização de qualquer ato de procedimento licitatório público; ter afastado ou procurado afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo; ter fraudado licitação pública ou contrato dela decorrente; ter criado, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo; ter obtido vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ter manipulado ou fraudado o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública; ter dificultado atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou ter intervindo em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização.

14.1.1. As práticas passíveis de rescisão, tratadas nesse inciso, podem ser definidas, dentre outras, como:

a) corrupta: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação do empregado da **CET** na execução do contrato;

b) fraudulenta: falsificar ou omitir fatos, com o objetivo de influenciar o processo de execução do contrato;

c) coercitiva: causar dano ou ameaçar, direta ou indiretamente, as pessoas físicas ou jurídicas, visando afetar a execução do contrato;

d) obstrutiva: destruir, falsificar, alterar ou ocultar provas ou fazer declarações falsas, com objetivo de impedir materialmente a apuração de práticas ilícitas.

14.1.2. As práticas exemplificadas no subitem **14.1.1.**, além de acarretarem responsabilidade administrativa, a ser apurada no curso do próprio processo administrativo de contratação, de acordo com o caso concreto, poderão implicar em responsabilidade civil indenizatória e/ou indenização na esfera criminal, nos termos da Lei.

14.2. Os casos de rescisão contratual devem ser formalmente motivados nos autos do processo, devendo ser assegurado o contraditório e o direito de prévia e ampla defesa.

CLÁUSULA DÉCIMA QUINTA - DO RECEBIMENTO DO OBJETO

15.1. O objeto do Contrato somente será recebido quando perfeitamente de acordo com as condições contratuais e demais documentos que fizerem parte do ajuste.

15.2. Executado o contrato, o seu objeto deverá ser recebido:

I - em se tratando de obras e serviços:

a) provisoriamente, pelo responsável por seu acompanhamento e fiscalização; ou

b) definitivamente, pelo Gestor do Contrato.

15.2.1. O recebimento provisório ou definitivo não exclui a responsabilidade civil, principalmente quanto à solidez e segurança da obra ou do serviço, nem ético profissional pela perfeita execução nos limites estabelecidos pelo Código Civil Brasileiro e pelo contrato.

15.2.2. Nos casos devidamente justificados, os prazos para recebimento provisório e definitivo poderão ser prorrogados mediante autorização da autoridade competente, formalizada através de Aditamento, desde que celebrado anteriormente ao término da vigência contratual.

15.2.3. Na hipótese de rescisão do contrato, caberá ao responsável pela fiscalização atestar as parcelas adequadamente concluídas, recebendo provisória ou definitivamente, conforme o caso.

CLÁUSULA DÉCIMA SEXTA - DA POSSIBILIDADE DE ALTERAÇÃO

16.1. Existe a a possibilidade de alteração do presente Instrumento, por acordo entre as partes, de acordo com o previsto nos incisos I a VI do art. 81 da Lei Federal nº 13.303/16 nos seguintes casos:

I - quando houver modificação do projeto ou das especificações, para melhor adequação técnica aos seus objetivos;

II - quando necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites permitidos por esta Lei;

III - quando conveniente a substituição da garantia de execução;

IV - quando necessária a modificação do regime de execução dos serviços, bem como do modo de fornecimento, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;

V - quando necessária a modificação da forma de pagamento, por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado, vedada a antecipação do pagamento, com relação ao cronograma financeiro fixado, sem a correspondente contraprestação de execução dos serviços;

VI - para restabelecer a relação que as partes pactuaram inicialmente entre os encargos do contratado e a retribuição da administração para a justa remuneração dos serviços, objetivando a manutenção do equilíbrio econômico-financeiro inicial do contrato, na hipótese de sobrevirem fatos imprevisíveis, ou previsíveis porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

CLÁUSULA DÉCIMA SÉTIMA - DA LEGISLAÇÃO APLICÁVEL

17.1. Lei Federal nº 13.303/16, Decreto Federal 10.024/19, Lei Complementar nº 123/06, com suas alterações, Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/18, alterada pela Lei nº 13.853/19 e ***Regulamento Interno de Licitações, Contratose Convênios - RILCC da CET***, aplicando-se, quando for o caso, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições do Direito Privado.

CLÁUSULA DÉCIMA OITAVA – DA PROTEÇÃO DE DADOS PESSOAIS

18.1 A **CONTRATADA** está ciente do inteiro teor da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais – LGPD) e se obriga a observar o dever de proteção de Dados Pessoais, proteger os direitos de privacidade, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, e se compromete a cumprir todas as condições e obrigações dispostas nas leis aplicáveis, em especial, nas Leis 13.709/18, 12.527/11 e 12.965/14.

18.1.1. A **CONTRATADA** não poderá se utilizar de informação, dados pessoais ou base de dados a que tenham acesso, para fins distintos da execução dos serviços especificados neste instrumento contratual.

18.2. A **CONTRATADA** deverá realizar o tratamento dos dados pessoais da **CET** em estrita observância aos princípios previstos no artigo 6º da LGPD, incluindo, mas não se limitando à finalidade, adequação, necessidade, transparência, livre acesso, segurança, prevenção, e não discriminação. A **CONTRATADA** compromete-se a realizar suas atividades de forma que os direitos dos titulares dos dados sejam respeitados e garantidos.

18.3. A **CONTRATADA** se responsabilizará por assegurar que todos os seus colaboradores, consultores, e/ou prestadores de serviços que, no exercício das suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, respeitem o dever de proteção, confidencialidade e sigilo, devendo estes assumir compromisso formal de preservar a confidencialidade e segurança de tais dados, documento que está disponível em caráter permanente para exibição a CET, mediante solicitação.

18.3.1. A **CONTRATADA** está obrigada a assumir total responsabilidade e efetuar o ressarcimento por todo e qualquer dano e/ou prejuízo sofrido, incluídas eventuais sanções aplicadas pela autoridade nacional decorrentes de tratamento inadequado dos dados pessoais compartilhados pela CET para as finalidades pretendidas neste contrato.

18.3.2. Eventuais responsabilidades serão apuradas de acordo com o que dispõe a Seção III, Capítulo VI da LGPD, **devendo qualquer intercorrência ser comunicada pelo gestor do contrato por meio do e-mail** encarregado_lgpd@cetsp.com.br

18.4. Os dados pessoais coletados pela **CONTRATADA** serão armazenados apenas pelo período necessário para o cumprimento das finalidades específicas do contrato, em conformidade com o artigo 15 da LGPD.

18.4.1. Após o término dos serviços contratados, se a devolução dos dados não for solicitada pela CET, os mesmos deverão ser eliminados de forma segura e permanente, exceto nos casos em que seja necessário manter os dados para o cumprimento de obrigação legal ou regulatória, conforme previsto no artigo 16, inciso I da LGPD.

CLÁUSULA DÉCIMA NONA – DAS DISPOSIÇÕES FINAIS E CONFIDENCIALIDADE

19.1 Para execução deste Contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção, seja de forma direta ou indireta quanto ao objeto deste contrato ou de outra forma a ele não relacionada, devendo garantir, ainda que seus prepostos e colaboradores ajam da mesma forma, nos termos do Decreto nº 56.633, de 24 de novembro de 2015.

19.2 A **CONTRATADA** concorda com as normas, políticas e práticas estabelecidas no **Código de Conduta e Integridade da CET,** disponível no site da CET/Transparência CET, no link: http://www.cetsp.com.br/media/719911/codigo-de-conduta-e-integridade-1a-rev.pdf, comprometendo-se com o seu integral cumprimento, inclusive por parte de seus empregados e prepostos, conforme previsto na Lei Federal nº 13.303/16 e no Decreto Municipal nº 58.093/18, comprometendo-se com a ética, dignidade, decoro, zelo e eficácia e os princípios morais que norteiam as atividades desempenhadas no exercício profissional e fora dele, em razão das obrigações contratuais assumidas, com foco na preservação da honra e da tradição dos interesses e serviços públicos.

19.3. A **CONTRATADA** concorda e compromete-se em cumprir as Normas de Segurança de Informações estabelecidas na CET, nos termos da Política de Segurança da Informação - PSI, disponível em http://www.cetsp.com.br/media/1177904/15-politica-de-seguranca-da-informacao-cet.pdf.

19.4. A **CONTRATADA** deverá manter sigilo absoluto sobre quaisquer dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob as penas da lei, independentemente da classificação de sigilo conferida a tais documentos, principalmente no que tange os DADOS PESSOAIS tratados.

19.5. A **CONTRATADA** não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da **CET,** sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

19.6 Nenhuma tolerância das partes quanto à falta de cumprimento de quaisquer das cláusulas do ajuste poderá ser entendida como aceitação, novação ou precedente.

CLÁUSULA VIGÉSIMA - DO FORO

20.1. Para solucionar quaisquer questões oriundas deste Contrato, é competente, por disposição legal, o foro da Fazenda Pública da Comarca da Capital, São Paulo.

E, por se acharem assim justas e contratadas, assinam o presente Contrato em 02 (duas) vias de igual teor e forma, diante das testemunhas abaixo indicadas, que também o assinam.

São Paulo, 20 de janeiro de 2025.

O ORIGINAL ASSINADO ENCONTRA-SE NO EXPEDIENTE Nº 0429/24

PREGÃO ELETRÔNICO Nº 043/2024

EXPEDIENTE Nº 0429/24

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM SERVIÇOS DE MONITORAMENTO E GERENCIAMENTO DE TRÁFEGO DA REDE DE DADOS DA COMPANHIA DE ENGENHARIA DE TRÁFEGO CET, COM MANUTENÇÃO E SUPORTE, POR UM PERÍODO DE 24 (VINTE E QUATRO) MESES.

ANEXO I

TERMO DE REFERÊNCIA

ASSUNTO: Solução para Monitoramento e gerenciamento de tráfego da Rede de Informática da Companhia de Engenharia de Tráfego - CET

Resumo: Está solução de monitoramento proporciona visibilidade no tráfego de pacotes de dados que trafegam na rede de dados da Companhia de Engenharia de Tráfego – CET, possibilitando a tomada de decisões para obter maior eficiência e uma segurança mais robusta.

1. OBJETO

1.1. Contratação de empresa especializada em serviços de Monitoramento e gerenciamento de tráfego da Rede da Companhia de Engenharia de Tráfego – CET com manutenção e suporte técnico em localizados na Rua Bela Cintra, 385, Consolação - São Paulo – SP e na Rua Sumidouro 740 Pinheiros, por um período de 24 (vinte e quatro) meses.

2. VIGÊNCIA DO CONTRATO

2.1. O Contrato a ser firmado terá um prazo de 24 (vinte e quatro) meses, podendo ser prorrogado até o limite da lei.

3. ESPECIFICAÇÕES TÉCNICAS

3.1. Características Técnicas Gerais

3.1.1. A solução para Monitoramento e gerenciamento de tráfego da Rede de dados da Companhia de Engenharia de Tráfego - CET deverá ser do tipo agregador de tráfego e ser oferecido em hardware suportando montagem em rack de 19” (dezenove polegadas), com utilização de no máximo dois (2) rack units de altura por Datacenter, com fornecimento dos respectivos conjuntos de fixação.

3.1.2. Deverá possuir funcionalidades e hardware específicos para este propósito de agregação, regeneração, filtragem e modificação/transformação do tráfego, não sendo aceitas soluções similares, como: switches, roteadores, firewalls, balanceadores, servidores, soluções híbridas e etc.

3.1.3. Deverão ser de um mesmo fabricante, incluindo os itens agregador, módulos, gerencia centralizada e GBICs, com vista ao não desperdício de recursos técnicos e facilidade de integração.

3.1.4. A solução de observabilidade de tráfego de rede pode ser de um fabricante diferente da solução de agregador de tráfego.

3.1.5. Deverá possibilitar a configuração dinâmica de portas via software, permitindo a definição de portas de rede, rede inline, ferramenta e portas de ferramenta inline.

3.1.6. Entende-se por portas de rede, todas as portas que serão responsáveis por receber a có-

pia do tráfego através dos Test Access Point ou Terminal Access Point (TAPs)/Switch port Analyzer (SPANs).

3.1.7. 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 agregação de tráfego.

3.1.8. Entende-se por portas de Rede inline, todas as portas que serão responsáveis por encaminhar o tráfego de produção.

3.1.9. 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 à solução.

3.1.10. Deverá possuir módulos de ventilação hot swappable.

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

3.1.12. Deverá possuir fonte de alimentação interna que trabalhe em 110V_240V, 50/60 Hz, com detecção automática de tensão e frequência, hot swappable.

3.1.13. Deverá suportar simultaneamente em sua memória flash, duas imagens do sistema operacional entregue com o equipamento.

3.2. Quantitativos

3.2.1. Deverão ser fornecidos, no mínimo, **dois (2) equipamentos agregadores de tráfego** com as seguintes características:

3.2.1.1. Quatro (4) interfaces de 10/100/1000 compatíveis com o padrão 1000BaseT, com licenciamento para ativação de todas essas portas;

3.2.1.2. Oito (8) interfaces de 10/100/1000 compatíveis com o padrão 1000BaseT, com capacidade de funcionamento em modo TAP/Bypass permitindo o encaminhamento de tráfego mesmo quando o equipamento está desligado e com licenciamento para ativação de todas essas portas;

3.2.1.3. Vinte e quatro (24) interfaces de 1/10Gbps compatíveis com os padrões SFP/SFP+, com licenciamento para ativação de todas essas portas;

3.2.1.4. Capacidade nominal de 20Gbps de processamento de tráfego inteligente;

3.2.1.5. Deverão ser fornecidas licenças para as seguintes funcionalidades de processamento inteligente de tráfego:

3.2.1.5.1. Deduplicação de pacotes.

3.2.1.5.2. Flow de rede enriquecido com metadados da camada de aplicação.

3.2.1.5.3. Application Aware.

3.2.2. Deverão ser fornecidos dispositivos utilizados para monitorar e capturar o tráfego de rede de dados de maneira passiva e não intrusiva sem interferir nas operações normais da rede, conhecidos como TAPs (Test Access Points) para interceptação de, no mínimo, vinte e quatro (24) links no padrão 1/10G LX/LR **monomodo para fibras com conector LC** com raio de divisão de 70/30, sendo doze (12) links no site Bela Cintra e doze (12) links no site Sumidouro.

3.2.3. Deverão ser fornecidos TAPs para interceptação de, no mínimo, vinte e quatro (24) links no padrão 1/10G SX/SR **multimodo para fibras com conector LC** com raio de divisão de 50/50, sendo doze (12) links no site Bela Cintra e doze (12) links no site Sumidouro.

3.2.4. Deverão ser fornecidos, no mínimo, dezesseis (16) transceivers de 1Gb Base1000T;

3.2.5. Deverão ser fornecidos, no mínimo, dezesseis (16) transceivers de 1Gb Base SX;

3.2.6. Deverão ser fornecidos, no mínimo, dezesseis (16) transceivers de 1Gb Base LX;

3.2.7. Deverão ser fornecidas licenças de software da solução de gerenciamento centralizada dos Network Packet Brokers e agregadores de tráfego dos TAPs em uma única

console central.

3.2.8. A solução deve considerar a instalação dos TAPs e agregadores de tráfego dos TAPs em dois prédios diferentes (Bela Cintra e Sumidouro).

3.2.9. Deverá ser fornecido todo o cabeamento necessário para a operacionalização da solução, incluindo fibras ótica, cabos UTP e quaisquer outros elementos necessários para viabilizar a interconexão entre:

3.2.9.1. TAPs de fibra ótica e elementos de rede existentes

3.2.9.2. TAPs e Network Packet Broker

3.2.9.3. Network Packet Broker e elementos de rede existentes

3.2.9.4. Network Packet Broker e servidores que rodam as soluções de monitoramento

3.2.10. Deverão ser considerados cabos com tamanho de 10 metros para interligação entre equipamentos instalados em racks diferentes.

3.2.11. Deverão ser considerados cabos com tamanho de 2 metros para interligação entre equipamentos instalados no mesmo rack.

Tabela 1: Compõem o objeto desta contratação os seguintes itens:

ITEM DESTE TERMO DE REFERÊNCIA	DESCRIÇÃO	QUANTIDADE
3.2.1	Máquina física (equipamentos agregadores de tráfego)	02
3.2.2	Dispositivos utilizados para monitorar e capturar o tráfego de rede de dados – TAPs (Test Access Points) no padrão 1/10G LX/LR **monomodo** para fibras com conector LC	24
3.2.3	Dispositivos utilizados para monitorar e capturar o tráfego de rede de dados – TAPs (Test Access Points) no padrão 1/10G SX/SR **multimodo** para fibras com conector LC	24
3.2.4	transceivers de 1Gb Base1000T	16
3.2.5	transceivers de 1Gb Base SX	16
3.2.6	transceivers de 1Gb Base LX	16
3.2.7	licenças de software da solução de gerenciamento centralizada dos Network Packet Brokers e agregadores de tráfego dos TAPs	02
4	Solução de Observabilidade de Rede	01
5	Detecção e Resposta à Ameaças em Rede	01
6	Treinamento	02
7	Suporte técnico prestados em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, por 24 meses	01

3.3. Gerenciamento

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

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

3.3.3. Deverá possuir suporte a MIB II.

3.3.4. Deverá implementar a MIB privativa que forneça informações relativas ao funcio-

namento do equipamento.

3.3.5. Deverá suportar SNMP trap sobre IPv6.

3.3.6. Deverá permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface de gerenciamento.

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

3.3.8. 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.

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

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

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

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

3.3.13. Deverá implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+, RADIUS e LDAP.

3.3.14. Deve suportar IPv4 e IPv6 para TACACS+.

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

3.3.16. Deverá proteger a interface de comando do equipamento através de senha.

3.4. Aplicação de Regras

3.4.1. 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:

3.4.1.1. Uma para uma.

3.4.1.2. Uma para várias - Com suporte ao balanceamento.

3.4.1.3. Várias para uma.

3.4.1.4. Várias para várias - Com suporte ao balanceamento.

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

3.4.2.1. Endereços MAC de origem e destino

3.4.2.2. Endereço IPv4 de origem/destino

3.4.2.3. Portas TCP e UDP de origem e destino

3.4.2.4. VLAN ID

3.4.2.5. Ethertype

3.4.2.6. IPFrag

3.4.2.7. TTL

3.4.2.8. TOS

3.4.2.9. Protocol

3.4.2.10. TCP Control Mask/Bits

3.4.2.11. DSCP

3.4.2.12. Versão do Protocolo IPv4 e IPv6

3.4.2.13. Endereço IPv6 de origem/destino

3.4.3. A solução deverá suportar, no mínimo, 16000 (dezesseis mil) filtros (regras) de entrada e saída.

3.4.4. 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.

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

3.4.6. A solução deverá implementar funcionalidade Mesh/Cluster.

3.4.7. O Mesh/Cluster deverá permitir a configuração e gerenciamento de 2 (dois) ou mais agregadores de tráfego como um único equipamento lógico. Não serão aceitas soluções em cascata para o atendimento desta funcionalidade.

3.4.8. A solução deverá suportar, no mínimo, 30 agregadores em modo Mesh/Cluster.

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

3.4.10. 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 equipamentos entre estes equipamentos. Não serão aceitas soluções em cascata para o atendimento deste item.

3.4.11. 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.

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

3.4.13. Deve permitir a configuração de circuitos entre mesh/clusters de agregadores, permitindo que o tráfego recebido em um cluster seja entregue para uma ferramenta em outro cluster.

3.5. Funcionalidades Inline

3.5.1. O equipamento deve suportar instalação sem necessidade de reconfiguração de roteadores e switches, quando utilizado no modo de operação Inline.

3.5.2. O equipamento deve suportar, de forma simultânea e em interfaces distintas, os modos:

3.5.2.1. TAP/SPAN (Cópia de Tráfego).

3.5.2.2. Inline (Tráfego de Produção).

3.5.3. 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 de tráfego funcionar de forma Inline.

3.5.4. O equipamento deverá permitir a configuração conjunta das funcionalidades Serial e Paralelo, permitindo criar uma sequência serial de ferramentas que estão em Paralelo.

3.5.5. O equipamento deverá permitir que ferramentas inline em modo standalone, serial e paralelo, possam ter a flexibilidade de receber somente o tráfego de interesse, sem impacto entre elas e sem a necessidade de workaround físico. Por exemplo, a ferramenta 1 precisa receber todo o tráfego e a ferramenta 2 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 da outra.

3.5.6. Suportar 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.

3.5.7. O equipamento 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.

3.5.8. O equipamento 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 agregação de tráfego. Caso este pacote retorne a ferramenta inline será considerada em falha e deverá ser removida sem impacto na rede e nos fluxos de dados.

3.5.9. A solução de agregação de tráfego, 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.

3.5.10. O equipamento de agregação de tráfego 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.

3.6. Funcionalidades Avançadas

3.6.1. Deverá ter Throughput de vinte (20) Gbps para processar as funcionalidades de Deduplicação.

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

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

3.6.4. A funcionalidade de Tunnel deve suportar o encapsulamento e o desencapsulamento utilizando protocolo L2GRE ou VXLAN, permitindo transportar o tráfego encapsulado através de diferentes redes L3.

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

3.6.6. Deve suportar a funcionalidade Packet Trimming (Corte do Pacote), otimizando o tráfego que será encaminhado para as ferramentas reduzindo o tamanho do pacote.

3.6.7. A funcionalidade de Packet Trimming deve ser configurável para cortar o pacote das seguintes formas:

3.6.7.1. Dinâmico, ou seja, a partir de um campo específico do cabeçalho ethernet definido pelo usuário.

3.6.7.2. Estático, ou seja, a partir de um offset específico definido pelo usuário.

3.6.8. A funcionalidade de Packet Trimming deve permitir que o corte de pacotes ocorra depois que a contagem de pacotes atingiu um valor configurado, evitando assim o corte de informações de controle e outros dados importantes dos protocolos de rede.

3.6.9. Deve suportar terminação Encapsulated Remote Switch Port Analyzer (ERSPAN), permitindo terminar um tráfego espelhado de equipamentos que suportam ERSPAN.

3.6.10. Deve suportar terminação ERSPAN para as versões II e III.

3.6.11. Deve suportar a funcionalidade Masking (Alteração de dados), que é capaz de modificar determinadas informações contidas no tráfego de rede antes de redirecioná-lo para as Ferramentas, para atendimento de normas de proteção de dados, quando necessário.

3.6.12. A funcionalidade Masking deverá ser capaz de trocar uma determinada informa-

ção como o CPF do usuário por outros caracteres, como por exemplo XXX.XXX.XXX-XX, de modo que essa informação específica seja protegida antes de ser enviada para os equipamentos de coleta e análise de fluxos e pacotes.

3.6.13. Deve suportar a funcionalidade Protocol Stripping (Remoção de Cabeçalho), permitindo identificar e remover TAGs de VLANs e cabeçalhos específicos dos pacotes de rede.

3.6.14. A funcionalidade de Protocol Stripping deve suportar a remoção de pelo menos os seguintes cabeçalhos:

3.6.14.1. VLAN.

3.6.14.2. MPLS.

3.6.14.3. VNTag.

3.6.14.4. VXLAN.

3.6.14.5. Fabric Path.

3.6.14.6. GRE.

3.6.14.7. ISL.

3.6.14.8. QinQ.

3.6.14.9. GTP.

3.6.15. A funcionalidade de Protocol Stripping também deverá suportar a remoção de cabeçalhos que não estejam pré-definidos, permitindo assim a customização de um offset e quantidade de bytes deverão ser removidos, permitindo assim a remoção de cabeçalhos não padronizados.

3.6.16. Deve implementar a funcionalidade Packet De-Duplication (Deduplicação de Pacotes), enviando somente uma única cópia do pacote para as ferramentas.

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

3.6.18. 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.

3.6.19. 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:

3.6.19.1. IPv4 ToS.

3.6.19.2. IPv6 TC.

3.6.19.3. Número de sequência TCP.

3.6.19.4. VLAN ID.

3.6.20. Deve implementar a funcionalidade de geração de flow de rede enriquecido com metadados da camada de aplicação.

3.6.21. Deve suportar o envio de metadados usando os protocolos IPFIX, Syslog, HTTP e HTTPS.

3.6.22. Deve implementar a geração de NetFlow nas versões v5 e v9 e IPFIX.

3.6.23. A geração de NetFlow/IPFIX/CEF deve suportar os seguintes métodos de amostragem:

3.6.23.1. Unsampled (Sem amostragem).

3.6.23.2. A configuração de Unsampled ou Sampled deverá ser configurável através da CLI e WEB (HTTPS).

3.6.24. Deve implementar a geração de, no mínimo, os seguintes metadados para prover informações superiores à da camada de rede, quando utilizando IPFIX/CEF:

3.6.24.1. HTTP Method.

3.6.24.2. HTTP Response Code.
3.6.24.3. HTTP Version.
3.6.24.4. HTTP Host.
3.6.24.5. HTTP URI.
3.6.24.6. HTTP RTT.
3.6.24.7. HTTP Request-ts.
3.6.24.8. HTTP Response-ts.
3.6.24.9. HTTP User-Agent.
3.6.24.10. DNS Query Name.
3.6.24.11. DNS Query Type.
3.6.24.12. DNS Response Code.
3.6.24.13. DNS Response TTL.
3.6.24.14. DNS Response Name.
3.6.24.15. DNS Tunneling.
3.6.24.16. SSL Certificate Issuer.
3.6.24.17. SSL Certificate CN.
3.6.24.18. SSL Version.
3.6.24.19. SSL Cipher Suite ID.
3.6.24.20. SSL Validity-Not-After.
3.6.24.21. SSL Validity-Not-Before.
3.6.24.22. RDP Version.
3.6.24.23. RDP Username ASCII.
3.6.24.24. RDP Encryption Level.
3.6.24.25. RDP Security Protocol.
3.6.24.26. TCP RTT.
3.6.24.27. TCP RTT App.
3.6.24.28. TCP Loss bytes.
3.6.24.29. TCP Retransmission bytes.
3.6.24.30. TCP Wrong CRC.

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

3.6.26. A funcionalidade DPA deve permitir a criação de filtros utilizando linguagem de programação Perl ou RegEx.

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

3.6.28. 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.

3.6.29. 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.

3.6.30. 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 em que o padrão da sessão for detectado após o handshake da sessão, todos os pacotes anteriores também sejam encaminhados para as Ferramentas.

3.6.31. 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).

3.6.32. A funcionalidade de filtragem por aplicação deve suportar a identificação de, no

mínimo, 3000 aplicações agrupadas por famílias ou grupos de aplicações tais como YouTube, Whatsapp e Gmail.

3.6.33. Deve suportar a definição regras baseadas em expressões regulares para aplicações customizadas, incluindo protocolos e extensões proprietárias.

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

3.6.35. Deve suportar a funcionalidade SSL Decryption através de função Man-In-The-Middle e também somente cópia do tráfego através de licenciamento adicional.

3.6.36. O equipamento deve suportar um throughput exclusivo de tráfego criptografado de, no mínimo, dois (2) Gbps.

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

3.6.38. O equipamento deve permitir importação de no mínimo 1.000 (hum mil) certificados em formato PKCS #12 ou PEM.

3.6.39. O equipamento deve suportar, no mínimo, os seguintes algoritmos de troca de chaves com autenticação:

3.6.39.1. RSA.

3.6.39.2. DHE_RSA.

3.6.39.3. ECDHE_RSA.

3.6.39.4. ECDHE_ECDSA

3.6.40. O equipamento deve suportar, no mínimo, os seguintes métodos de autenticação de mensagens:

3.6.40.1. SHA.

3.6.40.2. SHA256.

3.6.40.3. SHA384.

3.6.40.4. POLY1305.

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

3.6.42. A funcionalidade SSL Decryption deve suportar, no mínimo, os seguintes protocolos:

3.6.42.1. TLS 1.0

3.6.42.2. TLS 1.1

3.6.42.3. TLS 1.2

3.6.42.4. TLS 1.3

3.6.43. O equipamento deve suportar, no mínimo, as seguintes cifras de criptografia:

3.6.43.1. AES_128_CBC.

3.6.43.2. AES_256_GCM.

3.6.43.3. CHACHA20.

3.6.43.4. Camellia.

3.6.43.5. DES_CBC.

3.6.43.6. 3DES_EDE_CBC.

3.6.43.7. Chacha20-Poly1305.

3.7. TAPs de Fibra ótica Multimodo 1Gbps SX

3.7.1. Os TAPs monomodo deverão possuir os seguintes requisitos técnicos:

3.7.1.1. Deve via acompanhado dos acessórios para montagem em rack 19”, incluindo o chassi de instalação em rack, se necessário.

3.7.2. Deve possuir altura máxima de 1 RU (1,75").

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

3.7.4. Deve ser totalmente passivo, ou seja, não é necessário nenhum tipo de alimenta-

ção elétrica, software e configuração para o seu funcionamento.

3.7.5. Cada TAP deverá possuir 2 (duas) interfaces de rede, responsável por conectar os dispositivos de rede adjacentes;

3.7.6. Cada TAP deverá possuir 2 (duas) interfaces de monitoramento, responsável por enviar todo o tráfego TX e RX coletado entre os elementos adjacentes;

3.7.7. Deverá suportar conexões do tipo Multimodo 850nm para fibras com 50/125 microns, 1Gbps SX com conector LC e split ratio de 50/50.

3.8. TAPs de Fibra ótica Monomodo 1Gbps LX

3.8.1. Os TAPs monomodo deverão possuir os seguintes requisitos técnicos:

3.8.1.1. Deve via acompanhado dos acessórios para montagem em rack 19”, incluindo o chassi de instalação em rack, se necessário.

3.8.2. Deve possuir altura máxima de 1 RU (1,75").

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

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

3.8.5. Cada TAP deverá possuir 2 (duas) interfaces de rede, responsável por conectar os dispositivos de rede adjacentes;

3.8.6. Cada TAP deverá possuir 2 (duas) interfaces de monitoramento, responsável por enviar todo o tráfego TX e RX coletado entre os elementos adjacentes;

3.8.7. Deverá suportar conexões do tipo Monomodo 1310/1550nm, 1Gbps LX com conector LC e split ratio de 70/30.

3.9. Gerenciamento Centralizado

3.9.1. Deverá ser fornecido um software capaz de controlar, administrar, gerenciar e monitorar a solução de Visibilidade, com suporte a, no mínimo, 1000 ativos da solução de Visibilidade.

3.9.2. O software deverá estar licenciado para, no mínimo, 5 ativos físicos da solução de Visibilidade, e permitir upgrades através da aquisição de licença adicional.

3.9.3. A console de gerenciamento deve ser única e deve abranger todos os itens ativos e gerenciáveis da solução.

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

3.9.5. O software de gerenciamento poderá ser fornecido em forma de appliance virtual compatível com hypervisors VMware, Hyper-V ou KVM.

3.9.6. 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.

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

3.9.8. A solução deve possibilitar a configuração de diferentes perfis de administradores. Deve ser possível ainda criar usuários com perfil de administração e outros de apenas visualização.

3.9.9. Deve permitir a visualização da topologia da solução de visibilidade para todos os equipamentos ativos e gerenciáveis.

3.9.10. Deve permitir a identificação do status das portas dos dispositivos up ou down,

tecnologia e velocidade das portas.

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

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

3.9.13. 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.

3.9.14. Deve permitir o upgrade do sistema operacional dos dispositivos, individualmente e para um grupo de dispositivos, inclusive podendo agendar um dia e horário para que este upgrade aconteça automaticamente.

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

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

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

3.9.17.1. Total de portas que estão perdendo pacotes.

3.9.17.2. Total de portas acima do limite de utilização, tanto portas de Rede como portas de Ferramenta.

3.9.17.3. TOP portas com maior utilização.

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

3.9.18. A CONTRATANTE fornecerá infraestrutura para rodar a console de gerenciamento da solução de visibilidade de rede considerando uma (1) VM com os seguintes requisitos de hardware:

3.9.18.1. 16Gb (Giga bytes) de memória RAM

3.9.18.2. 200GB (Giga bytes) de disco de estado sólido (SSD)

3.9.18.3. 4 cores de processamento

3.9.18.4. 1 interface de rede exclusiva para gerência

4. Solução de Observabilidade de Rede

4.1. Requisitos de infraestrutura e hardware

4.1.1. O fornecimento da infraestrutura de servidores e necessários para funcionamento da solução de observabilidade de rede será de responsabilidade da CONTRATANTE.

4.1.2. O fornecimento da plataforma de virtualização necessários para funcionamento da solução de observabilidade de rede será de responsabilidade da CONTRATADA.

4.1.3. A plataforma de virtualização da CONTRATADA permitirá rodar máquinas virtuais (VMs) compatíveis com os sistemas operacionais baseados em Linux de 64 bits ou Windows Server 2022 (ou superior).

4.1.4. A CONTRATANTE fornecerá infraestrutura DE SERVIDORES para rodar até três (3) VMs com os seguintes requisitos de hardware:

4.1.4.1. 64Gb (Giga bytes) de memória RAM

4.1.4.2. 4TB (Tera bytes) de disco de estado sólido (SSD)

4.1.4.3. 8 cores de processamento

4.1.4.4. 2 interfaces de rede virtuais com velocidade mínima de 1Gbps UTP, sendo:

4.1.4.4.1. 1 interface exclusiva para gerência

4.1.4.4.2. 1 interface exclusiva para recebimento de eventos e logs

4.1.5. As máquinas virtuais (VMs) da solução de observabilidade de rede serão instalados no Datacenter principal da CONTRATANTE.

4.2. Busca e visualização dos dados

4.2.1. A solução deve fornecer recursos para pesquisa de texto completo (full-text search).
4.2.2. A solução deve permitir busca federada para visão unificada de dados armazenados em diferentes tenants e/ou ambientes (híbrido ou multinuvem).
4.2.3. A solução deve permitir a correlação de dados de diferentes camadas (logs, métricas, traces, eventos de segurança, entre outros) em um mesmo console, possibilitando uma investigação mais efetiva e análise da causa raiz (RCA).
4.2.4. A solução deve permitir o armazenamento e busca de dados geoespaciais.
4.2.5. A solução deve fornecer recurso de grafos para identificação de relacionamentos relevantes em dados e exploração de correlações.
4.2.6. A solução deve suportar a interação com os dados usando sintaxe da linguagem SQL.
4.2.7. A solução deve disponibilizar dashboards e gráficos prontos para uso.
4.2.8. A solução deve fornecer recursos para a construção de dashboards, gráficos e relatórios customizados.
4.2.9. A solução deve oferecer recursos para a criação de dashboards avançados e infográficos.
4.2.10. A solução deve fornecer recursos para análise e visualização de dados geoespaciais.
4.2.11. A solução deve fornecer recursos para restringir o acesso a objetos (dashboards e relatórios) de acordo com o perfil do usuário.
4.2.12. A solução deve permitir o compartilhamento e a exportação de objetos (dashboards e relatórios).
4.2.13. A solução deve possibilitar o uso de recursos interativos em dashboards, como filtros e drilldowns, permitindo o redirecionamento para outros painéis e sites externos.
4.2.14. A solução deve ser capaz de prover diferentes tipos de opções de agregação de dados para análise e sumarização, incluindo agregação de métricas, buckets e matrizes, incluindo suporte à agregações hierárquicas e geoespaciais.
4.2.15. A solução deve fornecer recursos para acelerar a identificação da causa raiz de problemas, como correlação de latência e erros em transações.
4.2.16. A solução deve suportar a interação com os dados usando sintaxe da linguagem SQL.
4.2.17. A solução deverá categorizar automaticamente as mensagens de logs, permitindo que o usuário identifique a frequência das mensagens de maneira rápida e amigável.
4.2.18. A solução deverá permitir que uma mensagem de log seja encontrada dentro de um contexto ou fluxo de mensagens, agilizando a investigação de um eventual problema.
4.2.19. A solução deverá permitir filtrar e organizar as mensagens de log por conjuntos customizados e datasets baseados nos serviços integrados à plataforma.
4.2.20. O conjunto de mensagens de logs deverá ser visualizável de maneira de stream (fluxo de dados) em tempo real, com a opção de pausar e continuar o Stream
4.2.21. Deverá ser possível visualizar uma linha do tempo dividida nas últimas 24 horas onde o usuário consiga escolher exatamente o ponto de análise dos logs.
4.2.22. Deverá ser possível destacar termos nos textos presentes dos logs ingeridos para

facilitar a investigação de um campo específico.

4.2.23. A plataforma deverá ser capaz de apresentar os logs em stream em diferentes tamanhos de texto e espaços de linhas.

4.2.24. A plataforma deverá ser capaz de realizar busca e queries dos logs de maneira constante e contínua durante a geração dos mesmos.

4.2.25. A solução deverá permitir que os logs sejam observáveis de maneira temporal com detalhamento de até milissegundos.

4.2.26. A solução deverá possuir em sua plataforma, como solução única e independente, a capacidade de detectar anomalias no fluxo de mensagens de log com pontuações (score), gráficos de calor e visualizações customizadas para diferentes urgências.

4.3. Recursos de machine learning

4.3.1. A solução deve oferecer recursos nativos de machine learning para aprendizado não supervisionado (detecção de anomalias, outliers e forecasting), supervisionado (classificação e regressão) e processamento de linguagem natural (NLP).

4.3.2. A solução deve oferecer modelos prontos para uso, com foco em AIOps, com capacidades de previsibilidade de recursos inclusos.

4.3.3. A plataforma deverá possuir recurso que identifique picos de ingestão de logs, entenda o comportamento do ambiente e analise a motivação de tais picos como funcionalidade integrada.

4.3.4. A plataforma deverá possuir recurso que identifique padrões de logs de forma automática, como conteúdo dos campos do dos logs ingeridos e sua frequência diante do volume total presente no armazenamento.

4.3.5. A solução deve suportar a importação e o uso de modelos externos.

4.3.6. Os modelos deverão ser filtrados por tipo, criação, descrição e outros detalhes.

4.3.7. Os modelos poderão ter versões, sendo presentes na plataforma e facilitando o controle para estudos com os logs

4.3.8. A plataforma deverá possuir suporte à visualização da estimativa de operações necessárias para cada modelo treinado integrado

4.3.9. A plataforma deverá possuir funcionalidade que permita eventual teste do modelo treinado de maneira amigável em assistente existente com dados anteriormente ingeridos ou processados no momento do teste

4.3.10. A solução deve permitir a identificação de anomalias, sem a necessidade de duplicação dos dados.

4.3.11. A solução deverá apresentar uma console onde seja possível visualizar os recursos utilizados dedicados aos processos de Machine learning

4.3.12. A solução deverá possuir visualização consolidada da quantidade de documentos processados para cada rotina (job) criado com o conteúdo presente no armazenamento

4.3.13. A solução deverá ser capaz de filtrar jobs que estão em funcionamento, concluídos e outras informações como:

4.3.13.1. Identificação da rotina de machine learning

4.3.14. Tipo de rotina de machine learning

4.3.15. Versão da plataforma e das funcionalidades utilizadas

4.3.16. Data de criação e de conclusão da rotina

4.3.17. Identificação do modelo utilizado

4.3.18. Grupos e descrição da rotina de machine learning e seu funcionamento

4.3.19. Informações do ciclo de vida dos dados do modelo utilizado

4.3.20. Quantidade de bytes que foram utilizados para determinar os resultados do modelo

4.3.21. Quantidade de dados inválidos de datas e campos que não são compatíveis com o modelo
4.3.22. Script em JSON com a estrutura das informações e configurações específicas da rotina explorada
4.3.23. A solução deverá permitir o acesso às mensagens com seus respectivos timestamps dos nós envolvidos na rotina criada
4.3.24. A solução deve permitir a criação de rotinas de machine learning através de ferramentas que facilitem a experiência do usuário como assistente de configuração.
4.3.25. A solução deverá suportar a criação de rotinas com objetivos específicos como:
4.3.25.1. Rotinas que detectam anomalias utilizando uma única métrica
4.3.25.2. Rotinas que detectam anomalias utilizando uma ou mais métricas sendo capazes de separar durante a análise
4.3.25.3. Rotinas que detectam atividade não usual em uma população para dados com alta cardinalidade
4.3.25.4. Rotinas de categorização de logs customizadas para novas detecções de anomalias
4.3.25.5. Rotinas para detecção de valores raros em um dado de série temporal
4.3.25.6. Rotinas de detecção de anomalias com dados em localidades geográficas variadas
4.3.25.7. Rotinas avançadas com a combinação de metodologias diferentes para casos de uso mais específicos
4.3.26. O assistente de configuração deverá descrever cada passo e demonstrar as possibilidades de utilização dos campos
4.3.27. A solução deverá permitir escolher o intervalo de tempo necessário para compor a amostra ingerida pela rotina para o aprendizado de máquina (bucket span)
4.3.28. O assistente de configuração das funcionalidades de machine learning deverá realizar a validação dos campos e configurações inseridos nos passos anteriores antes de consumir os recursos computacionais necessários para a rotina, permitindo que o usuário valide se a análise está dentro do esperado e se existem recursos para tal.
4.3.29. A plataforma deverá permitir que, mesmo que uma análise seja montada e programada, possa ser iniciada em outro momento, tendo seus parâmetros armazenados e sem necessidade de repetição de inserção dos valores.
4.3.30. O assistente de configuração deverá permitir que a rotina criada possa ser convertida em uma rotina avançada antes de ser iniciada.
4.3.31. A plataforma deverá demonstrar uma visualização estimada dos dados que serão utilizados para a análise com visualizações sugeridas como gráficos de dois eixos, por exemplo.
4.3.32. A solução deverá permitir a visualização focada com o viés de machine learning nos dados ingeridos, facilitando possíveis futuras análises dos mesmos.
4.3.33. A solução deverá permitir a integração de calendários para que as rotinas sejam filtradas de maneira automatizada e suportem eventos planejados como janelas de manutenção, feriados, entre outros, evitando que os logs ingeridos contaminem a detecção de anomalias.
4.3.34. A solução deverá permitir a configuração de filtros para as rotinas permitindo incluir ou excluir eventos específicos das análises utilizando machine learning.
4.3.35. A solução deverá permitir que os resultados sejam exportados e explorados em outros dashboards dentro da mesma plataforma, facilitando a análise posterior.
4.3.36. A solução deverá possuir funcionalidade de detecção de ponto de mudança automática, sendo possível configurar a função necessária, campo de métricas e campo adicional para obter a análise detalhada do comportamento do ambiente.

4.3.37. A solução deverá possuir visualização consolidada de notificações relacionadas às análises e rotinas de machine learning ativas ou passadas.

4.3.38. A solução deverá possuir integração nativa com APIs de IA Generativa como ChatGPT e AWS Bedrock para auxílio na identificação e resolução de alertas relacionados à performance da aplicação.

4.4. Integrações e notificações

4.4.1. A solução deve permitir a configuração de alertas, especificando condições para execução de ações predefinidas.

4.4.1.1. A solução deverá disponibilizar uma visualização consolidada dos alertas, incluindo alertas ativos e resolvidos.

4.4.1.2. A solução deverá, em sua configuração de alertas, ser capaz de ativar ou desativar a detecção de alertas que alteram constantemente entre ativos e resolvidos para evitar alertas desnecessários para a equipe usuária.

4.4.1.3. A configuração de alertas que alteram constantemente deve ser possível dentro da customização de vezes que as regras foram ativadas e que o estado do alerta foi alterado, permitindo que isso seja alterado durante todo o período de contrato da solução.

4.4.1.4. A configuração dos alertas deverá ser baseada em regras criadas dentro da própria plataforma e, assim que elas forem cumpridas, o alerta será gerado.

4.4.1.5. A configuração dos alertas deverá possuir campo de customização de nome.

4.4.1.6. A configuração dos alertas deverá permitir a utilização de tags para identificação.

4.4.1.7. A configuração dos alertas deverá permitir filtro por caso de uso como logs de diferentes ambientes, métricas e logs de infraestrutura.

4.4.1.8. A configuração dos alertas deverá permitir a customização de scripts com campos como fonte dos logs, quantidade dos logs, nível dos logs, condições, intervalo de tempo, agrupamento, entre outros.

4.4.1.9. A plataforma deverá permitir a definição do intervalo de checagem da regra em segundos, minutos, horas e dias.

4.4.2. A solução deve fornecer integrações para notificação de alertas via e-mail, IBM Resilient, Jira, Microsoft Teams, Opsgenie, PagerDuty, ServiceNow, Slack, Swimlane, Tines, Webhook e xMatters.

4.4.2.1. Para cada tipo de integração, a plataforma deverá ser capaz de customizar as ações referentes aos conectores de maneira individual e independente.

4.4.2.2. A plataforma deverá permitir que mais de uma ação seja tomada, incluindo mais de uma integração como resultado de um alerta (enviar um e-mail e abrir um caso no ServiceNow com o mesmo alerta, por exemplo).

4.4.3. A solução deve fornecer recurso para alertar quando um objeto em movimento cruzar um limite geográfico predefinido (geofencing).

4.4.4. A solução deve possibilitar o início de tarefas corretivas, previamente automatizadas, a partir de um ou mais alertas, previamente definidos, automaticamente, através de integração com webhooks.

4.4.5. A solução de ingestão de logs deve analisar o comportamento de todos os itens refletidos no escopo com filtros de tempo e permitindo comparações e buscas entre os campos

4.4.6. A plataforma de ingestão deve permitir que os dados ingeridos não necessitem filtro o conversão de formato para que sejam analisados de maneira detalhada

4.4.7. A plataforma deverá possuir funcionalidade de criação e gerenciamento de chamados baseados em dados ingeridos no ambiente, permitindo integrações com

ferramentas externas como Jira e ServiceNow

4.4.7.1. A criação de chamado dentro da plataforma deve permitir configurações de campos como tags para identificação, severidade do chamado, e permitir descrição com linguagem markdown para melhor integração de outras formas de evidências.

4.4.7.2. A severidade do chamado criado dentro da plataforma deverá possuir as seguintes opções: Baixa, Média, Alta e Crítica.

4.5. Licenciamento e posicionamento no mercado

4.5.1. A solução proposta deve possuir modelo de licenciamento flexível e baseado no uso de recursos (total de memória alocado para instâncias do cluster e DTS), sem cobrança por volume de ingestão, número de usuários, agentes de coleta, aplicações, quantidade de requisições ou documentos.

4.5.2. A solução proposta deve fornecer suporte 24x7x365.

4.5.3. Tempo de resposta para chamados críticos:

4.5.3.1. Severidade 1: 1 hora

4.5.3.2. Severidade 2: 4 horas

4.5.3.3. Severidade 3: 1 dia

5. Detecção e Resposta à Ameaças em Rede:

5.1. Características Gerais

5.1.1. Deve ser construída a partir da premissa de que a ameaça já está presente dentro do ambiente da organização e utilize o tráfego da rede como fonte para identificar os rastros deixados pelos adversários.

5.1.2. Deve gerar metadados (dados sobre dados) a partir do tráfego de rede analisado, enviar tais metadados para o repositório de dados na nuvem ou on-premises, permitindo a rápida consulta e contextualização das ameaças no ambiente da organização.

5.1.3. Deve permitir que a organização implemente um processo de investigação, threat hunting e forense de rede com base em metadados da solução utilizando funcionalidades de detecção e investigação.

5.1.4. Deve permitir que os analistas de segurança façam a triagem e investigação sobre os eventos de rede e criem buscas usando o resultado das consultas anteriores como ponto de partida afim de identificar comportamentos maliciosos complexos.

5.1.5. Deve ser alimentada por mais de 100 fontes de inteligência de ameaças, incluindo pesquisa interna, fontes comerciais, comunidades Open Source e entidades de setores específicos como indústria e governo.

5.1.6. Deve ser aderente ao framework de segurança cibernética ATT&CK do Mitre.

5.1.7. Deve ser ofertada como um modelo de serviço SaaS (Software as a Service) onde o fornecedor é responsável pela implantação e manutenção da plataforma, enquanto a organização é responsável pelos acessos e utilização.

5.1.8. Deve possuir sensores que serão instalados na rede da organização para coletar, processar e gerar metadados a partir do tráfego de rede.

5.1.9. Deve ser licenciada com base no volume de tráfego recebido pelos sensores instalados na rede da organização e não pelo número de sensores.

5.1.10. Deve ser escalável e não sofrer degradação de desempenho em função do grande volume de dados coletados, processados e armazenados.

5.1.11. A solução deverá ser fornecida inicialmente com capacidade de inspeção agregada

de, no mínimo, 500 Mbps.

5.1.12. Com o objetivo de maximizar a compatibilidade e simplificar o gerenciamento, a solução deve ser do mesmo fabricante da solução de visibilidade de rede.

5.2. Requisitos de infraestrutura e hardware

5.2.1. O fornecimento da infraestrutura de servidores necessários para funcionamento da solução de detecção de ameaças rede será de responsabilidade da CONTRATANTE.

5.2.2. O fornecimento da infraestrutura de plataforma de virtualização necessários para funcionamento da solução de detecção de ameaças rede será de responsabilidade da CONTRATADA.

5.2.3. A plataforma de virtualização da CONTRATADA permitirá rodar máquinas virtuais (VMs) compatíveis com os sistemas operacionais baseados em Linux de 64 bits ou Windows Server 2022 (ou superior).

5.2.4. A CONTRATANTE fornecerá infraestrutura para rodar até duas (2) VMs com os seguintes requisitos de hardware:

5.2.4.1. 16Gb (Giga bytes) de memória RAM

5.2.4.2. 500GB (Giga bytes) de disco de estado sólido (SSD)

5.2.4.3. 4 cores de processamento

5.2.4.4. 2 interfaces de rede virtuais com velocidade mínima de 1Gbps UTP, sendo:

5.2.4.4.1. 1 interface exclusiva para gerência

5.2.4.4.2. 1 interface exclusiva para recebimento da cópia de tráfego da rede

5.2.5. As máquinas virtuais (VMs) da solução de detecção de ameaças de rede serão instalados em duas localidades diferentes, sendo uma (1) VM no site Bela Cintra e uma (1) VM no site Sumidouro.

5.3. Gerenciamento e repositório de dados:

5.3.1. Deve possuir uma interface de gerenciamento acessada de forma segura via protocolo HTTPS, utilizando criptografia forte.

5.3.2. Deve possuir uma interface simples de usar que suporte a revisão das detecções, a triagem dos eventos, as investigações e a condução de operações de buscas por ameaças.

5.3.3. Deve suportar a criação dashboards customizáveis incluindo, mas não se limitando, gráficos, visões de linha de tempo, detecções e cobertura dos sensores.

5.3.4. Deve suportar a criação dashboards parametrizáveis que permitam a organização determinar rapidamente quais hosts se comunicaram com um domínio, quando se comunicaram, quais portas foram utilizadas e o volume de dados trafegados em uma única visão.

5.3.5. Deve suportar autenticação baseada em múltiplos fatores incluindo, mas não se limitando, o Google MFA.

5.3.6. Deve suportar a criação de tokens de acesso para consumo da API da solução.

5.3.7. Deve suportar a integração com sistemas de autenticação externos baseados em SAML SSO.

5.3.8. Deve permitir a criação de usuários com diferentes perfis de acesso, incluindo no mínimo, administrador, usuário e usuário somente-leitura.

5.4. Sensores:

5.4.1. Devem suportar o recebimento de cópias do tráfego de rede através do uso de tecnologias como SPAN, TAP ou NPB.

5.4.2. Devem suportar uma implantação zero-touch, onde os sensores são enviados para o ambiente da organização já devidamente configurados e prontos para utilização.
5.4.3. Devem ser oferecidos através de um modelo de serviço, onde a organização contratante não tenha responsabilidade sobre a instalação, configuração e manutenção dos mesmos.
5.4.4. Devem possuir interface de gerenciamento dedicada e que possua conectividade com a Internet para enviar os metadados coletados para o repositório de dados na nuvem.
5.4.5. Devem possuir interface para recepção das cópias de tráfego de rede do ambiente.
5.4.6. Devem permitir que a interface de gerenciamento fique em uma rede segregada no ambiente da organização, sem comunicação com os demais hosts internos.
5.4.7. Apenas metadados relevantes para a detecção e investigação de ameaças devem ser submetidos para a nuvem, nenhum dado de identificação pessoal ou informação privada deve ser coletado.
5.4.8. Deve possuir sensores virtuais para diferentes tipos de ambiente, incluindo no mínimo:
5.4.8.1. VMWare
5.4.8.2. HyperV
5.4.8.3. KVM
5.4.8.4. AWS
5.4.8.5. Azure

5.5. Detecções:

5.5.1. Deve ser constantemente alimentada por assinaturas de detecção de ameaças construídas por um time de pesquisa de ameaças avançadas do fornecedor.
5.5.2. Tais assinaturas devem ser focadas nas táticas, técnicas e procedimentos dos adversários ao invés de apenas indicadores atômicos (tais como endereços IP, hash de arquivos, entre outros).
5.5.3. As detecções gerenciadas pelo fornecedor da solução devem possuir as respectivas informações de severidade e nível de confiabilidade, incluindo o curso de ação inicial que deve ser tomado pela organização como resposta para a detecção.
5.5.4. A solução deve permitir que a própria organização crie assinaturas customizadas baseado em indicadores de comprometimento (IoC) e com base no resultado de pesquisas relevantes aos seus ambientes.
5.5.5. A solução deve ser capaz de identificar atividades maliciosas sendo realizadas por um atacante dentro dos vários estágios da cadeia de ataque, incluindo as tentativas de exploração de vulnerabilidades, a transferência de artefatos maliciosos para o ativo atacado, a movimentação lateral entre ativos na rede interna, a comunicação de comando e controle (C2) e o vazamento de dados para a Internet.
5.5.6. Deve permitir que a organização defina regras de exceção para endereços IP específicos para que as atividades de análise de vulnerabilidades ou testes de invasão não gerem falso-positivos.
5.5.7. Deve suportar a definição das faixas de endereçamento IP interno da organização.
5.5.8. Deve suportar o agrupamento das detecções em diferentes categorias, tais como:
5.5.8.1. Aplicações potencialmente maliciosas
5.5.8.2. Postura de segurança
5.5.8.3. Ataques
5.5.9. Deve suportar o envio de notificações das detecções realizadas por e-mail.
5.5.10. Deve suportar o envio de um resumo diário das detecções por e-mail.
5.5.11. Deve suportar a filtragem dos e-mails de notificações enviados pela solução com

base na severidade, nível de confiança, categoria das detecções ou outras classificações similares.

5.5.12. Deve permitir que regras de detecção específicas não gerem e-mails de notificação.

5.5.13. Deve permitir que a organização faça a resolução das detecções utilizando classificações específicas tais como mitigado, falso positivo ou similares.

5.5.14. Deve suportar a resolução manual e automática das detecções com base na configuração das respectivas regras.

5.5.15. Deve suportar a criação de uma lista de exclusão para que não sejam geradas detecções para dispositivos específicos.

5.6. Investigações:

5.6.1. Deve possuir uma funcionalidade que permita ao analista manter o controle dos passos realizados durante uma investigação, com espaço para anotações e observações.

5.6.2. Deve permitir que o analista crie consultas manualmente sobre o histórico do tráfego.

5.6.3. Deve possuir uma funcionalidade de playbooks que permita a execução de trabalhos investigativos repetitivos de forma simplificada, sem a necessidade de criação de consultas manuais.

5.6.4. A funcionalidade de investigação deve permitir a execução de diferentes consultas de forma paralela e simultânea.

5.6.5. A solução deve enriquecer os dados sobre as entidades de rede (hosts) com informações que facilitem o curso da investigação, tais como:

5.6.5.1. Entidade responsável pelo IP com base no serviço who.is.

5.6.5.2. Geolocalização do endereço IP.

5.6.5.3. Reputação do IP ou de indicadores relacionados no Vírus Total.

5.6.5.4. Monitoramento passivo de DNS.

5.6.5.5. Usuários autenticados através de NTLM ou Kerberos.

5.6.5.6. Softwares identificados com base no tráfego monitorado.

5.6.6. Deve permitir o armazenamento de consultas comuns para que sejam reutilizadas em investigações futuras.

5.6.7. Deve suportar a busca por entidades de rede (hosts) e os respectivos eventos de rede associados.

5.6.8. Deve permitir a busca por eventos de forma retroativa com base no histórico dos metadados gerados a partir do tráfego de rede.

5.6.9. Deve suportar a adição de blocos de indicadores (por exemplo, uma lista de endereços IP maliciosos) na funcionalidade de busca, para identificar eventual comunicação maliciosa.

5.6.10. Deve suportar a retenção dos metadados para fins de investigação e busca retroativa por no mínimo 365 (trezentos e sessenta e cinco) dias de forma online.

5.6.11. A solução deverá processar o tráfego e armazenar os metadados das comunicações realizadas na plataforma de dados da solução.

5.6.12. Deve oferecer uma linguagem de consultas rica e estruturada, permitindo que a organização faça a pesquisa por indicadores de ameaças e entenda rapidamente a cadeia de eventos que leva aos incidentes de segurança.

5.6.13. Deve possuir a capacidade de detecção retroativa, permitindo que seja feita a análise histórica do tráfego da rede para identificar a presença de ameaças, usando indicadores e consultas recém-criadas.

5.6.14. Deve possuir funcionalidade de busca por indicadores de ameaças com tempo de

resposta muito baixo para as consultas, permitindo a redução no tempo médio de remediação.

5.6.15. Deve permitir a extração de arquivos executáveis a partir do tráfego de rede e realizar a análise estática sobre os mesmos para identificar arquivos maliciosos em trânsito.

5.6.16. Deve ser implantado através de um modelo de serviço de gerenciado, da implantação até a operação no dia a dia, sendo a configuração e manutenção da solução gerenciada pelo próprio fornecedor.

5.6.17. Deve suportar a criação de gráficos dinâmicos das entidades e hosts da rede, permitindo a identificação de comportamentos anômalos.

5.6.18. Deve suportar o processamento e geração de metadados para os seguintes tipos de eventos:

5.6.18.1. Flow – Conexões de rede na camada IP
5.6.18.2. DNS – Requisições DNS
5.6.18.3. HTTP – Requisições HTTP
5.6.18.4. SMTP – Requisições de e-mail SMTP
5.6.18.5. SSL – Conexões SSL
5.6.18.6. X.509 – Certificados
5.6.18.7. Requisições Kerberos
5.6.18.8. Transferência de arquivos PE (Portable Executable)
5.6.18.9. RDP – Sessões de RDP
5.6.18.10. SSH – Sessões de SSH
5.6.18.11. DHCP – Eventos de servidor ou cliente DHCP
5.6.18.12. SURICATA – Eventos de detecção baseados em Suricata
5.6.18.13. Arquivo SMB – Transferência de arquivos usando o protocolo SMB
5.6.18.14. Mapeamento SMB – Mapeamento de conexão SMB
5.6.18.15. Softwares detectados a partir do tráfego de rede
5.6.18.16. NTLM – Requisições do protocolo NTLM
5.6.18.17. FTP – Transferência de arquivos via FTP
5.6.18.18. DCE-RPC – Eventos do protocolo DCE-RPC

5.6.19. Deve permitir identificar se o evento de rede bateu com uma ou mais fontes de inteligência de ameaças.

5.7. Dispositivos:

5.7.1. Deve permitir a visualização da quantidade de dispositivos identificados pelos sensores da solução ao longo do tempo.

5.7.2. Deve suportar a visualização do percentual de dispositivos em cada sub-rede que fazem comunicações internas e externas à organização.

5.7.3. Deve suportar a verificação de que a solução está recebendo o tráfego dos dispositivos de rede.

5.7.4. Deve suportar a identificação das faixas de endereçamento IP e as respectivas sub-redes com base no tráfego recebido pela solução.

5.8. Captura de Tráfego:

5.8.1. Deve suportar a geração de captura de tráfego de forma seletiva para enriquecer as atividades de Threat Hunting.

5.8.2. Deve suportar a criptografia dos arquivos PCAP gerados a partir da captura seletiva para preservar a confidencialidade das informações utilizando criptografia de chaves públicas.

5.8.3. Deve permitir rodar até 4 solicitações ativas de captura por sensor, sendo prioriza-

das por ordem de data/hora de solicitação.

5.8.4. Deve suportar a captura de até 1MB de tráfego por arquivo.

5.8.5. Deve suportar o encerramento automático da captura após 60 minutos do seu início, desde que o tráfego não tenha ultrapassado o limite de 1MB.

5.8.6. Deve permitir que a organização encerre a captura do tráfego manualmente.

5.8.7. Deve suportar a filtragem da captura do tráfego por endereços IP e portas.

5.8.8. Deve suportar o download do arquivo PCAP a partir da sua interface web para abertura em ferramentas externas de análise de tráfego (Ex: Wireshark).

5.9. API:

5.9.1. Deve possuir uma API RESTful permitindo a integração com sistemas de automação e orquestração de segurança existentes, aumentando a visibilidade sem incorrer em aumento do esforço operacional.

5.9.2. A API deve estar totalmente documentada, incluindo exemplos de requisições e respostas para cada API disponibilizada em formato JSON.

5.10. Integrações:

5.10.1. Deve suportar integração nativa ou via API com soluções de SOAR.

5.10.2. Deve suportar integração nativa ou via API com soluções de SIEM.

5.10.3. Deve suportar integração nativa ou via API com soluções de EDR.

5.10.4. Deve suportar integração nativa ou via API com fontes de Threat Intelligence de terceiros.

5.11. Time de Pesquisa de Ameaças:

5.11.1. A solução deve ser alimentada por fontes de inteligência de ameaças devidamente qualificadas por um time de pesquisas especializado, minimizando falso-positivos.

5.11.2. Devem fazer a curadoria das assinaturas e dos feeds de inteligência, permitindo que a organização gaste menos tempo com detecções de baixa qualidade e mais tempo na investigação de ameaças reais.

5.11.3. Os dados de inteligência revisados pelo time de pesquisa de ameaças devem permitir a análise da rede em tempo real, verificando a presença de indicadores de comprometimento (IoC) conhecidos.

5.11.4. O especialista técnico designado provê suporte contínuo para a organização na utilização da solução, suportando a criação de buscas customizadas, criação de relatórios técnicos e executivos e entendimento da necessidade da organização.

6. Servicos de Instalação

6.1. A CONTRATADA deverá garantir que todos os equipamentos, softwares, componentes, acessórios e cabos de conexão para interligar fisicamente a solução sejam entregues;

6.2. A CONTRATADA deverá assegurar a instalação de todos os softwares e ferramentas que acompanham a solução ofertada;

6.3. Para todos os produtos (hardware e software) disponibilizados pela Contratada, deverão ser fornecidos a instalação, a customização, a montagem física dos equipamentos e seus respectivos acessórios, bem como toda a configuração lógica;

6.4. Todas as configurações serão realizadas em conformidade com a recomendação do fabricante dos equipamentos e softwares da solução;

6.5. O equipamento ofertado deverá ser instalado e configurado na estrutura de rede LAN (Local Area Network) da CONTRATANTE, conforme parâmetros a serem definidos

em conjunto com a Contratada;

6.6. Todas as configurações deverão utilizar as boas práticas de implementação recomendada pelo fabricante e os requisitos de ambiente fornecidos pelo CONTRATANTE;

6.7. A instalação e configuração de cada componente deverá ser realizada por empresa autorizada pelo fabricante das soluções propostas;

6.8. A CONTRATADA será responsável pela qualidade dos serviços prestados;

6.9. A CONTRATADA deverá entregar serviços profissionais executados diretamente pelos fabricantes ou empregar técnicos certificados por eles para a execução dos serviços;

6.10. Fornecer todos os acessórios, trilhos, cabos, fibras e quaisquer materiais adjacentes para que possa ser concluída a instalação completa deles;

6.11. Os serviços de instalação e implementação deverão ser executados de forma a não comprometer os ambientes de produção durante o período de funcionamento da CET, ou seja, de segunda a sexta, das 7 às 19 horas:

6.11.1. Deverá ser realizada uma reunião de alinhamento on-site, ou remoto caso combinado entre as partes, para discutir os processos da instalação, em até 10 (dez) dias após a assinatura do contrato.

6.11.2. A contratada deverá elaborar o plano de testes e Validação, em conjunto com os técnicos da CET, em até 10 dias após a instalação dos equipamentos constantes do objeto. Os testes deverão ser executados de forma a não comprometer os ambientes de produção durante o período de funcionamento da CET, ou seja, de segunda a sexta, das 7 às 19 horas;

6.11.3. A entrega do material gerado dessa reunião deverá ser entregue em até 5 dias, para validação pelos técnicos da CET.

6.12. As atividades de instalação e configuração da solução devem ser realizadas localmente no site da CONTRATANTE a menos que seja acordado diferente entre as partes;

6.13. A CONTRATADA deverá fornecer a última versão disponível das licenças de uso dos softwares ofertados, observando as características, condições, quantidades e especificações constantes do Termo;

6.14. A CONTRATADA deverá entregar e executar um documento, aprovado pela CONTRATANTE, para a realização dos serviços de instalação, configuração e migração do ambiente, contendo ao menos os seguintes itens:

6.14.1. Cronograma de todas as atividades a serem realizadas;

6.14.2. Documentação de toda a migração realizada;

6.14.3. Documentação do tipo As-built com diagramas da arquitetura e resultados de todas as configurações executadas durante os procedimentos de instalação da nova solução;

6.14.4. Realização de testes completos visando a garantia da disponibilidade e validação do ambiente como um todo, demonstrando estabilidade nas aplicações existentes, após toda a instalação, configuração e migração;

6.14.5. Configuração inicial conforme recomendação do fabricante;

6.14.6. Deverá ocorrer sem quaisquer ônus a CONTRATANTE.

6.15. Correrão por conta da CONTRATADA as despesas com o frete, transporte, seguro e demais custos advindos da entrega dos produtos;

6.16. A CONTRATANTE, após o recebimento do As-Built, fará a emissão do Termo de Recebimento Definitivo (TRD);

6.17. A CONTRATADA deverá entregar qualquer componente da solução, a partir da assinatura do contrato, em até 60 (sessenta) dias corridos. Atrasos na entrega serão aceitos mediante condições extraordinárias e deverão ser avisados com antecedência máxima de até 15 (quinze) dias corridos prévios ao limite do prazo;

6.18. A CONTRATADA deve realizar o planejamento e "site survey" detalhado, incluindo indicação das atualizações necessárias aos ambientes operacionais em produção, para que a solução seja suportada;

6.19. Deverão ser realizadas as seguintes atividades mínimas para a solução de visibilidade do tráfego de rede:

6.19.1. Instalação física do sistema no Datacenter da CONTRATANTE: montagem em rack, energização, testes e verificação do perfeito funcionamento, com elaboração de relatório para comprovação dos testes, no Datacenter da Contratante;

6.19.2. Configuração Inicial do sistema, incluindo configuração de acesso de gerenciamento; ao sistema (usuários e senhas).

6.19.3. A CONTRATADA deve realizar a instalação dos Softwares envolvidos, incluindo testes e verificação do perfeito funcionamento.

7. Treinamento e capacitação

7.1. A CONTRATADA deverá prover 2 turmas de treinamento completo da solução ofertada para duas (2) turmas para 5 (cinco) colaboradores da CONTRATANTE.

7.2. Cada turma do treinamento deverá ser uma carga horária mínima de trinta e duas (32) horas.

7.3. O treinamento deve conter todo o conteúdo necessário para que as equipes da CONTRATANTE sejam capacitadas para administrar a solução bem como realizar customizações em suas configurações e instalar novos scanners/agentes e realizar integrações com ferramentas de terceiros. O treinamento deverá capacitar os participantes a realizar as seguintes atividades:

7.3.1. Operação da solução completa

7.3.2. Arquitetura da solução, módulos, componentes, integrações etc.

7.4. Os treinamentos devem ser ministrados por um profissional devidamente qualificado e certificado nos produtos que compõem a solução.

7.5. As sessões de treinamento podem ser ministradas de forma presencial ou remota. Caso o treinamento seja ministrado presencialmente devem ser consideradas sessões na cidade de São Paulo – SP.

7.6. Em caso de treinamento presencial, a CONTRATADA será responsável por providenciar o ambiente físico com a devida infraestrutura para a realização do treinamento, incluindo:

7.6.1. Mesas e cadeiras

7.6.2. Projetor

7.6.3. Computadores com conexão de Internet para realização dos laboratórios

7.7. A CONTRATADA deverá fornecer certificado de participação de cada treinamento para todos os participantes.

7.8. Os treinamentos devem ser compostos por exposição de conteúdo teórico e exercícios práticos em laboratório.

7.9. Todos os participantes dos treinamentos devem poder realizar os exercícios práticos de laboratório de forma individual.

7.10. Todos os participantes devem receber o material dos treinamentos contendo todo o conteúdo teórico exposto assim como a descrição de todos os exercícios práticos realizados em laboratório.

7.11. Deve haver lista de presença a ser assinada por todos os participantes de cada dia dos treinamentos.

7.12. Deve haver um formulário de avaliação dos treinamentos a ser preenchido e assinado por todos os participantes.

8. Suporte técnico prestados em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana

8.1. A CONTRATANTE, durante toda a vigência contratual, deverá permitir chamados ilimitados para o suporte técnico;
8.2. A contratada assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio da CONTRATANTE ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando da execução demandadas pela contratante;
8.3. Os representantes da CONTRATADA deverão se apresentar sempre com identificação visível, através de identidade profissional e/ou crachá da empresa;
8.4. A CONTRATADA deverá arcar com as despesas decorrentes dos deslocamentos de seus representantes, quando relacionados com a execução do contrato;
8.5. A CONTRATADA deverá se responsabilizar pelos atos cometidos pelos seus representantes na execução do contrato que possam causar danos a CET e a terceiros, decorrentes de sua culpa ou dolo, obrigando-se a reparar os danos causados;
8.6. Toda e qualquer atividade referente a configurações, ajustes, e outras parametrizações, que ocorrerem posteriormente à fase de implantação, serão precedidas da abertura de um chamado técnico;
8.7. A critério do CONTRATANTE, quando não houver necessidade de atendimento presencial, o serviço poderá ser prestado remotamente, e deverá cobrir todo e qualquer defeito apresentado, ajustes, reparos e correções necessárias para o perfeito estado de funcionamento da solução;
8.8. Sempre que requerido pelo CONTRATANTE, a CONTRATADA deverá apresentar declaração formal constando que ela continua sendo parceira do fabricante da solução ofertada e que ainda possui capacidade técnica e operacional para execução do objeto deste Termo de Referência;
8.9. Caso a atividade ocorra de modo proativo, a CONTRATADA informará a CONTRATANTE o motivo da execução tempestiva das ações através de e-mail;
8.10. Nos casos em que alguma atividade do serviço necessite da parada da solução, o CONTRATANTE deverá ser imediatamente notificado para que se proceda com a autorização, ou para que seja agendada nova data, a ser definida pela CONTRATANTE;
8.11. Todas as atualizações que envolvam indisponibilidade do ambiente devem ser agendadas com a equipe técnica da CONTRATANTE;
8.12. A CONTRATADA deverá possuir Central de Atendimento em português (brasileiro) para abertura de chamados e demais comunicações pertinentes, em regime 24x7x365;
8.13. A CONTRATANTE poderá solicitar a execução de serviços específicos através de canais de comunicação, como:
8.13.1. E-mail;
8.13.2. Contato Telefônico via 0800 ou DDD 11 (custo de ligação local);
8.13.3. Sistema de Chamados Web.
8.14. A CONTRATANTE considerará efetivamente realizado o serviço quando houver confirmação por sua área técnica da conclusão satisfatória do atendimento;
8.15. Todas as solicitações técnicas somente poderão ser encerradas com a anuência da CONTRATADA e do CONTRATANTE;
8.16. A CONTRATADA manterá cadastro das pessoas indicadas pelo CONTRATANTE que poderão efetuar a abertura e fechamento das solicitações de serviço;
8.17. Todo atendimento técnico presencial deverá ser registrado através de relatórios técnicos detalhados;

8.18. O término do atendimento não poderá ultrapassar o prazo estipulado para os diferentes níveis de criticidade;
8.19. Considera-se suporte técnico On-Site as atividades que devem ser executadas de forma presencial e acompanhadas por funcionário da CONTRATANTE;
8.20. A CONTRATADA deverá iniciar o atendimento de acordo com os prazos estipulados para o nível de criticidade. O início do prazo para o atendimento é o mesmo para os tipos de suporte On-site e Remoto;
8.21. Todo atendimento deverá ter o solicitante identificado, e ser limitado aos membros indicados da equipe do CONTRATANTE;
8.22. Atendimento desde o início até a sua conclusão deverá ser em idioma português;
8.23. Termos técnicos específicos e textos técnicos poderão ser usados em idioma inglês;
8.24. A Contratada deverá prestar os serviços de manutenção, com aparelhamento e ferramentas próprios, e técnicos com especialização, devidamente identificados;
8.25. O suporte técnico consiste no restabelecimento do funcionamento correto das soluções cobertas por esta contratação, assim como suas funcionalidades, através de um conjunto de ações e atividades (de configuração) que permitam a habilitação, a implementação/aplicação, a manutenção e a colocação em produção de quaisquer funcionalidades destes dispositivos;
8.26. A manutenção corretiva compreende os serviços para o restabelecimento do perfeito funcionamento dos equipamentos, com fornecimento de peças, de acordo com as especificações do fabricante, quando da ocorrência de quaisquer falhas ou defeitos nos componentes de hardware;
8.27. Manutenção Proativa:
8.27.1. Além do atendimento de CHAMADOS TÉCNICOS, a CONTRATADA deverá realizar MANUTENÇÃO PROATIVA, com atualização da solução e análise do ambiente e de todos os componentes da solução, com periodicidade máxima semestral, com detalhamento das ações e agendamento prévio;
8.27.2. A CONTRATADA fará monitoração contínua de eventos com abertura automática de chamados para eventuais problemas identificados e envio de notificação para o CONTRATANTE;
8.27.3. A CONTRATADA deverá fornecer sob solicitação do CONTRATANTE os seguintes relatórios em idioma português:
8.27.3.1. Todas as atualizações da solução em períodos solicitados;
8.27.3.2. Relação de incidentes ocorridos e solucionados com detalhamento;
8.27.3.3. Avaliação de tendências de falhas e recomendações preventivas;
8.27.3.4. Prestação de informações sobre o contrato (quantidade de licenças, tempo, entre outros).
8.27.4. Os relatórios acima podem ser entregues nos prazos a serem definidos pelo CONTRATANTE, via correio eletrônico em endereço a ser definido, ou disponibilizados em site web.
8.28. Caso haja necessidade de atualização de firmware dos componentes, a CONTRATADA deve providenciar o pacote de software e efetuar o serviço de atualização;
8.29. Fica facultado à equipe técnica da CONTRATANTE o fornecimento de acesso remoto para atendimento do tipo suporte, em caso em que os problemas identificados permitam esse tipo de atuação;
8.30. Abertura de chamados técnicos:
8.30.1. O sistema de abertura de chamados técnicos da CONTRATADA deverá registrar, no mínimo, as seguintes informações: data e hora da abertura e do fechamento do chamado técnico, identificação do solicitante, do problema e da solução;
8.30.2. Em caso de alteração do método ou meio de abertura de chamado técnico, a CON-

TRATADA informará o CONTRATANTE com antecedência mínima de 05 (cinco) dias úteis;

8.30.3. A existência de um chamado técnico, independentemente da sua fase de atendimento, não deverá restringir a abertura de novos chamados técnicos;

8.30.4. A abertura de um novo chamado técnico não deverá implicar no encerramento, ou suspensão, de outro chamado técnico que esteja aberto aguardando para ser atendido ou em fase de atendimento.

8.31. Os chamados técnicos serão classificados por GRAU DE SEVERIDADE, de acordo com o impacto no ambiente da CET:

8.31.1. Severidade 1: quando ocorre a perda ou paralisação de serviços relevantes prestados pela CONTRATANTE ou atividades exercidas por ela, configurando-se como emergência. Emergências devem ser tratadas com severidade 1 onde o atendimento deve ser realizado de forma presencial, ou remoto quando possível. Uma solicitação de serviço de Severidade 1 pode possuir uma ou mais das seguintes características:

8.31.1.1. Equipamento corrompido;

8.31.1.2. Uma função crítica do equipamento não está disponível;

8.31.1.3. O equipamento se desliga repentinamente causando demoras excessivas e intermitências para utilização de recursos;

8.31.1.4. O equipamento falha repetidamente após tentativas de reinicialização;

8.31.1.5. Falha crítica de componente do equipamento.

8.31.2. Severidade 2: quando se verifica uma grave perda de funcionalidade, no entanto, sem interromper os serviços prestados pela CONTRATANTE ou atividades exercidas por ela;

8.31.3. Severidade 3: quando se verifica uma perda de menor relevância de funcionalidades, causando apenas inconveniências para a devida prestação dos serviços pela CONTRATANTE ou a realização de atividades exercidas por ela;

8.31.4. Severidade 4: – quando solicitado criação de regras customizáveis nas soluções que não dependem de tal ação para a devida operação da CONTRATANTE ou atividades exercidas por ela;

8.31.5. Severidade 5: quando se verifica como necessária a prestação de informações, aperfeiçoamentos ou esclarecimentos sobre documentação ou funcionalidades, porém sem prejudicar diretamente a devida prestação dos serviços pela CONTRATANTE ou a realização de atividades exercidas por ela.

8.32. O nível de severidade será atribuído pela CONTRATANTE no momento da abertura do chamado;

8.33. Os chamados técnicos deverão ter resolução do problema técnico diagnosticado no atendimento técnico com restabelecimento do ambiente ao seu modo normal de operação em um prazo de:

8.33.1. Severidade 1:

8.33.1.1. 4 (quatro) horas corridas, contadas a partir da abertura do CHAMADO TÉCNICO, já incluso o tempo de deslocamento eventualmente necessário.

8.33.2. Severidade 2:

8.33.2.1. 12 (doze) horas corridas, contados a partir da abertura do CHAMADO TÉCNICO.

8.33.3. Severidade 3:

8.33.3.1. Próximo dia útil, contado a partir da abertura do CHAMADO TÉCNICO.

8.33.4. Severidade 4:

8.33.4.1. 3 (três) dias úteis, contados a partir da abertura do CHAMADO TÉCNICO.

8.34. Considerando a solução de ocorrências de hardware, caso se esgote o prazo de solução da ocorrência, sem que seja sanado o defeito reclamado, a CONTRATADA de-

verá providenciar a substituição do equipamento ou módulo defeituoso, em caráter definitivo dentro do prazo máximo de 24 (vinte e quatro) horas úteis. Após a substituição, a CONTRATADA deverá entregar um documento onde constem as descrições e os números de série dos módulos ou equipamentos defeituosos e de substituição;

8.35. Em caso de substituição definitiva de hardware, o equipamento deverá ser novo e original, recomendado pelo fabricante, com configuração igual ou superior à do equipamento substituído;

8.36. Durante a substituição definitiva a CONTRATADA deverá entregar um documento referente à substituição do equipamento pelo equipamento de substituição definitivo. Neste documento deverão constar a descrição e o número de série do equipamento defeituoso, a descrição e o número de série do equipamento de substituição definitivo;

8.37. Para fins de cálculo do período decorrido para solução da ocorrência de hardware, será contabilizado o prazo entre a formalização e o fechamento efetivo da ocorrência. Nos casos em que houver a substituição do módulo ou equipamento defeituoso para a solução da ocorrência, o seu fechamento efetivo se dará somente após a entrada em operação do novo módulo ou equipamento (de substituição).

9. DA HABILITAÇÃO TÉCNICA

9.1. A licitante deve apresentar, como condição para habilitação no certame, atestado de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, que comprove:

9.1.1. Que a Licitante desenvolveu e implantou projeto de segurança com características semelhantes aos descritos neste Termo de Referência.

9.1.2. Que a Licitante desenvolveu e implantou projeto de solução de agregador de tráfego.

9.1.3. Que a licitante desenvolveu e implantou projeto com fornecimento de no mínimo um agregador de tráfego

9.2. Os atestados de capacidade técnica apresentados deverão conter, no mínimo, Nome do Declarante, Endereço e Telefone e CNPJ da empresa emitente e a comprovação de que os serviços prestados atendem aos requisitos de qualidade estabelecidos

9.2.1. Caso a empresa Licitante não seja a fabricante dos produtos ofertados, esta deverá comprovar que está autorizada a comercializar as licenças de software ofertadas. Esta comprovação poderá ser mediante documento do fabricante ou impressão de página do site do fabricante comprovando a parceria.

9.3. DA EQUIPE TÉCNICA

9.3.1. A CONTRATADA se obriga a selecionar, designar e manter profissionais cuja qualificação esteja em conformidade com os tipos de serviços contratados observando as linguagens, ferramentas ou tecnologias a serem implementadas com o acompanhamento desta.

10. DAS PENALIDADES

10.1. Pelo descumprimento das obrigações assumidas a **CONTRATADA** estará sujeita às penalidades de advertência e multas/sanções a seguir especificadas e cujo cálculo tomará por base o valor do Contrato nas mesmas bases do ajuste, com fundamento no Capítulo II, Seção III, art. 82 da Lei Federal nº 13.303/16 e Capítulo XIII do Regulamento Interno de Licitações, Contratos e Convênios – RILCC da **CET**, garantindo o contraditório e a ampla e prévia defesa:

10.1.1. ADVERTÊNCIA para os casos, a seguir especificados, de atrasos, descumprimento ou apresentação de falhas nas obrigações contratuais e sempre que forem constatadas irregularidades de pouca gravidade e que o ato praticado pela **CONTRATADA**, ainda que ilícito, não seja suficiente para acarretar danos à **CET** e seus funcionários, suas instalações, imagem, meio ambiente ou a terceiros e que não justifique a imposição de sanção mais gravosa.

10.1.1.1. Não cumprimento do prazo estabelecido no ***subitem 6.11.1*** deste **Termo de Referência,** para a realização de reunião de alinhamento on-site ou remoto, por responsabilidade da **CONTRATADA.**

10.1.1.2. Não cumprimento do prazo estabelecido no ***subitem 6.11.2*** deste **Termo de Referência,** para a elaboração do plano de testes e validação, em conjunto com os técnicos da **CET**, após a instalação dos equipamentos constantes do objeto e/ou se os testes forem realizados comprometendo os ambientes de produção, durante o período de segunda a sexta-feira, das 07h00 às 19h00**.**

10.1.1.3. Não cumprimento do prazo estabelecido no ***subitem 6.11.3*** deste **Termo de Referência,** para a entrega do material gerado em decorrência da reunião prevista no ***subitem 6.11.1.***

10.1.1.4. Não atendimento dos prazos para os chamados técnicos relacionados aos Níveis de Severidade 3 e 4 estabelecidos nos ***subitens 8.33.3 e 8.33.4*** deste **Termo de Referência,** respectivamente.

10.1.2. Se, após a notificação de advertência pela **CET,** não ocorrer as entregas especificadas nos ***subitens 6.11.1 a 6.11.3, 8.33.3 e 8.33.4*** deste **Termo de Referência,** será aplicada multa de 10% (dez por cento) do valor mensal do contrato.

10.1.3. Persistindo a situação descrita na ***Cláusula 10.1.2*** após a aplicação da multa, fica caracterizada Inexecução Parcial do Contrato, com aplicação da penalidade correspondente.

10.1.4. O não cumprimento do prazo de 60 (sessenta) dias corridos da assinatura do contrato, estabelecido ***no item 6.17*** deste **Termo de Referência**, para a entrega dos componentes da solução, sem justificativas da **CONTRATADA** que caracterizem condições extraordinárias, acarretará multa de 10% dos valores correspondentes aos ***itens 3.2.1 a 3.2.7*** da ***Tabela 1*** deste **Termo de Referência**. Se, após a aplicação da penalidade não ocorrer a entrega, ficará caracterizada Inexecução Total do Contrato, com aplicação da penalidade correspondente.

10.1.5. O não atendimento do prazo para os chamados técnicos relacionados aos Níveis de Severidade 1 e 2 estabelecidos nos ***subitens 8.33.1 e 8.33.2*** deste **Termo de Referência,** acarretará multa de 10% (dez por cento), por dia de atraso, sobre o valor mensal do contrato referente ao Suporte técnico ***(item 7 da Tabela 1),*** até o limite máximo de 10 (dez) dias corridos, quando será caracterizada inexecução parcial do contrato, com aplicação da penalidade correspondente.

10.1.6. Multa de 5% (cinco por cento) sobre o valor contratual mensal, quando, sem justa causa aceita pela **CET,** a **CONTRATADA** não cumprir com qualquer outra obrigação assumida em decorrência do Contrato.

10.1.7. Pelo inadimplemento total ou parcial deste Contrato, independentemente da rescisão, a **CONTRATADA** ficará sujeita a critério da **CET** às seguintes penalidades:

10.1.7.1. Multa de 10% (dez por cento), por inexecução parcial do Contrato, mediante competente justificativa, **sobre o valor da parcela não executada**, nos termos do Art. 193, V do Regulamento Interno de Licitações, Contratos e Convênios - RILCC da CET.

10.1.7.2. Multa de 20% (vinte por cento), por inexecução total do Contrato, mediante competente justificativa, **sobre o valor total do Contrato**, nos termos do Art. 193, VI do Regulamento Interno de Licitações, Contratos e Convênios - RILCC da CET.

10.1.7.3. A inexecução parcial ou total do Contrato poderá ensejar sua rescisão nos termos do artigo nº 182 do Regulamento Interno de Licitações, Contratos e Convênios - RILCC da CET.

11. DA SUBCONTRATAÇÃO

11.1. Será aceita a subcontratação exclusivamente para o fornecimento de licenças de software e a compra de hardware de mercado.

11.1.1. O fornecimento poderá ser subcontratado somente após a autorização da **CET** e a **CONTRATADA** será responsável pelos mesmos.

Gerência de Informática - GIN