



**Governo do Estado de São Paulo**  
**Companhia Paulista de Trens Metropolitanos**  
**Depto De Contratações E Compras Por Meio Eletrônico**  
**CARTA**

CT.DFCE 0533/2024

Srs.

Neiva Maria da Silva / Francisco Augusto Zanet

Procuradores

INGRAM MICRO BRASIL LTDA

Rua Porto Alegre, 307 - Galpão 01 Módulo 01 e 02A Setor Parte A Setor Área EU V CIVIT II -  
Nova Zelândia

Serra – ES

CEP 29175-706

CONTRATO Nº RP00124-02 – Designação de Gestor

Prezados Senhores,

Comunicamos a V.Sas. que o Sr. Leonardo Marques Lopes, Chefe do Departamento de Operação de TI - DFIO, telefone (011) 3689-6328, será o responsável pela gestão do contrato em referência.

Sua função será a de coordenar os trabalhos, servindo de ligação entre V.Sas. e esta Companhia, na administração de problemas, tomando decisões técnicas e administrativas, dentro dos limites contratuais.

Atenciosamente,

CAMILO DOS SANTOS VASCONCELOS

Chefe do Departamento de Contratações e Compras por Meio Eletrônico



Documento assinado eletronicamente por **Camilo Dos Santos Vasconcelos, Chefe De Departamento**, em 30/12/2024, às 10:13, conforme horário oficial de Brasília, com fundamento no [Decreto Estadual nº 67.641, de 10 de abril de 2023](#).



A autenticidade deste documento pode ser conferida no site

[https://sei.sp.gov.br/sei/controlador\\_externo.php?](https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0) , informando o código verificador **0051272162** e o código CRC **5244FA08**.

**CONTRATO DE AQUISIÇÃO DE  
SOLUÇÃO DE PROTEÇÃO DE REDES  
NGFW – NEXT GENERATION  
FIREWALL FIRMADO ENTRE A  
COMPANHIA PAULISTA DE TRENS  
METROPOLITANOS - CPTM E A  
INGRAM MICRO BRASIL LTDA**

Pelo presente contrato, de um lado, a **COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM**, com sede no município de São Paulo, estado de São Paulo, na Rua Boa Vista, 185, inscrita no CNPJ/MF sob n.º 71.832.679/0001-23, doravante designada simplesmente **CONTRATANTE** e, de outro, a empresa **INGRAM MICRO BRASIL LTDA**, inscrita no CNPJ/MF sob n.º 01.771.935/0010-25, com sede na Rua Porto Alegre, 307 - Galpão 01 Módulo 01 e 02A Setor Parte A Setor Área EU V CIVIT II - Nova Zelândia - Serra – ES, doravante designada simplesmente **CONTRATADA**, representadas por seus representantes legais ao final designados e assinados, têm entre si justo e acertado o contrato de aquisição de solução de Proteção de Redes NGFW – NEXT GENERATION FIREWALL, mediante as seguintes cláusulas e condições:

## **I - OBJETO**

1.1. Constitui objeto do presente contrato a aquisição de solução de proteção de redes com característica de Next Generation Firewall - NGFW tipo 4, compreendendo Firewall, Módulo Transceptor, Cordão óptico, Pacote de licenças, Instalação do Firewall, ora denominados **PRODUTOS**, conforme detalhado no Termo de Referência - Anexo I do Edital, e demais condições estabelecidas neste contrato.

1.1.1. Os produtos estão descritos no item 2.1. SOLUÇÃO DE FIREWALL TIPOS 1, 2, 3, 4, 5 e 6 do Termo de Referência – Anexo I.

1.2. A forma de fornecimento do objeto contratado é integral por local.

1.3. A presente contratação, decorrente de licitação na modalidade Pregão Eletrônico n.º 077/2023, através da Ata de Registro de Preços n.º 001/2024, promovida pela COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO – PRODESP, foi homologada, assim como autorizada a previsão de despesa orçamentária no Documento de Comprovação Orçamentária – DCO, nos termos do Decreto Estadual n.º 33.144, de 20/3/91, conforme documentos anexados no Processo n.º SEI/SP- 359.00001160/2023-10.

## **II – PRODUTOS**

2.1. Todos os **PRODUTOS** deverão ser novos, sem uso anterior e deverão estar em linha de produção, sem previsão de encerramento na data de entrega da proposta, e o software/firmwares deverá ser fornecido em sua versão mais atualizada, conforme Termo de Referência - Anexo I.

2.1.1. A **CONTRATANTE** reserva-se o direito de rejeitar os **PRODUTOS** ou componentes que denotem uso anterior.



2.1.2. Os Produtos devem atender as condições estabelecidas nos itens 3, 4, 5, 6, 7, 8, 9 e 10 e respectivos subitens do Termo de Referência – Anexo I, a saber:

Item 3 - Características comuns a todos os Firewalls;

Item 4 - Características de Gerências;

Item 5 - Requisitos mínimos de Firewall;

Item 6 - Requisitos mínimos – Gerência;

Item 7 - Transceptores e cabos;

Item 8 - Garantia e Assistência Técnica;

Item 9 - Serviço de Instalação;

Item 10-Serviço de Treinamento.

2.1.3. A **CONTRATADA** deverá fornecer juntamente com os **PRODUTOS**, toda a documentação técnica original, completa e atualizada, contendo os manuais e guias de utilização, não sendo aceitas cópias de qualquer tipo, podendo ser disponibilizada em meio eletrônico original do fabricante.

### **III – ENTREGA**

- 3.1. Os **PRODUTOS** deverão ser entregues no endereço da **CONTRATANTE**, na Rua Zuma de Sá Fernandes, 360 – Osasco - SP, de segunda-feira a sexta-feira, das 08h30 às 11h30 e das 13h30 às 16h30.
- 3.2. A **CONTRATADA** deverá entregar os **PRODUTOS**, de acordo com a quantidade de cada item, indicados no Anexo II, em conformidade com os respectivos prazos de entrega estabelecidos no Termo de Referência - Anexo I, contados da data de assinatura deste contrato.
- 3.3. O prazo máximo para entrega dos **PRODUTOS** é de 90 (noventa) dias a contar da data de assinatura do Contrato o qual será emitido pela **CONTRATANTE** em nome da **CONTRATADA**.
- 3.4. A **CONTRATANTE** deverá ser comunicada com antecedência de 1 (um) dia, da data de realização da entrega, pela **CONTRATADA**.

### **IV – SERVIÇO DE INSTALAÇÃO**

- 4.1. Para a execução dos serviços de instalação, montagem física dos produtos e acessórios fornecidos, bem como a configuração lógica de todos os equipamentos e softwares envolvidos, a **CONTRATADA** deverá cumprir rigorosamente todas as condições e prazos estabelecidos no Termo de Referência - Anexo I deste contrato.
- 4.2. Os **PRODUTOS** serão instalados no âmbito do Estado de São Paulo: Região Metropolitana de São Paulo.
- 4.3. A instalação dos **PRODUTOS** deve ter início, no máximo, até 15 dias após a entrega.
- 4.4. A instalação dos **PRODUTOS** deverá ocorrer no prazo máximo de 30(trinta) dias úteis a contar da solicitação pela **CONTRATANTE**.

## **V – GARANTIA E ASSISTÊNCIA TÉCNICA/COMUNICAÇÕES E REGISTROS DE OCORRÊNCIAS**

- 5.1. A **CONTRATADA** deverá prestar os serviços de garantia “on site” para os **PRODUTOS** contratados, dispondo de canal de comunicação, cumprindo rigorosamente todas as condições e prazos de cobertura estabelecidos no Termo de Referência - Anexo I.
- 5.2. Todos os **PRODUTOS** deverão possuir garantia e assistência técnica pelo período de 60 meses do Fabricante, para cada tipo de Firewall, contado a partir do aceite da instalação.

## **VI – FORNECIMENTO, RECEBIMENTO E ACEITE**

- 6.1. O objeto contratado será fornecido, recebido e aceito em conformidade com as condições e prazos estabelecidos no Termo de Referência - Anexo I.

## **VII - OBRIGAÇÕES DA CONTRATADA**

- 7.1. Cumprir todas as condições estabelecidas neste contrato e no Termo de Referência – Anexo I.
- 7.2. Manter, durante toda a execução deste contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
- 7.3. Não emitir e/ou fazer circular duplicatas ou saque de letras de câmbio contra a **CONTRATANTE**, relativamente a todo e qualquer crédito decorrente deste contrato, exceto em se tratando a contratada de microempresa ou empresa de pequeno porte.
- 7.4. Responsabilizar-se pela entrega dos **PRODUTOS** contratados, bem como todas as despesas de transportes, fretes e seguros correspondentes.
- 7.5. Arcar com todas as despesas de reparos e/ou substituição dos **PRODUTOS**, contra defeitos de fabricação apresentados, durante o período de garantia.
- 7.6. Providenciar, concomitante à assinatura do contrato, seu cadastro na Unidade Cadastradora do Estado de São Paulo - CAUFESP, caso não esteja cadastrada ou sua renovação, caso esteja com o cadastro vencido, bem como mantê-lo válido durante toda a vigência contratual.
- 7.7. Obriga-se, por seus administradores, sócios e gerentes, por seus funcionários ou terceiros contratados e/ou subcontratados, credenciados e representantes, a manter e guardar o mais expresso, estrito e absoluto sigilo sobre dados, informações, conteúdo, especificações técnicas, características de ambientes, relações ou informações de caráter comercial com clientes da **CONTRATANTE**, a que tenham acesso ou conhecimento, sob qualquer forma, em decorrência da prestação dos serviços e/ou fornecimento de bem, objeto deste contrato, no decorrer da sua execução ou cumprimento, sob pena de responder civil e criminalmente pelo seu descumprimento, ficando responsável pela reparação por prejuízos materiais, morais, perdas e danos e lucros cessantes decorrentes.

- 7.7.1. A obrigação de sigilo prevista no item 7.7., aplica-se não só pelo prazo de vigência ou de execução dos serviços/fornecimento previstos neste contrato como se estende também após seu encerramento pelo prazo de 10 (dez) anos.
- 7.8. Observada a natureza do objeto contratado, responsabilizar-se exclusivamente, pela retirada e descarte do material até o destino final, sempre que solicitado pela **CONTRATANTE**, obrigando-se a apresentar a documentação comprobatória de sua qualificação para tanto, de conformidade com a legislação pertinente, sob pena de rescisão do ajuste, bem como da imposição das penalidades nele previstas.
- 7.9. Como condição para assinatura do presente contrato, caso a **CONTRATADA**, esteja em situação de recuperação judicial, deverá apresentar declaração, relatório ou documento equivalente de seu administrador judicial, ou se o administrador judicial for pessoa jurídica, do profissional responsável pela condução do processo, de que está cumprindo o plano de recuperação judicial e, caso a **CONTRATADA** esteja na situação de recuperação extrajudicial, deverá apresentar comprovação documental de que está cumprindo o plano de recuperação extrajudicial.
- 7.10. Assinar o "Termo de Ciência e de Notificação – Tribunal de Contas do Estado de São Paulo" - Anexo III deste contrato, dando ciência da remessa da documentação do procedimento licitatório ao Tribunal de Contas do Estado de São Paulo.
- 7.10.1. Providenciar o cadastro de seus representantes legais responsáveis pela assinatura do "Termo de Ciência e de Notificação" no Cadastro Corporativo TCESP – CadTCESP e mantê-lo atualizado, para fins de cadastramento em processo eletrônico, nos termos das Instruções nº 01 de 2020, alteradas pela Resolução nº 11 de 2021, do Tribunal de Contas do Estado de São Paulo.
- 7.10.2. Ficará a critério da **CONTRATADA** o acompanhamento do processo junto àquela corte, cabendo-lhe as diligências para juntada da procuração nomeando seus representantes legais/procuradores e demais atos que se fizerem necessários.
- 7.11. Assinar ao término da vigência do presente contrato, o Termo de Encerramento e Outras Avenças, conforme modelo Anexo IV deste contrato.

### **VIII - OBRIGAÇÕES DA CONTRATANTE**

- 8.1. Indicar o gestor do contrato, para acompanhar e fiscalizar a execução do presente contrato.
- 8.2. Efetuar os pagamentos conforme disposto na Cláusula X – FATURAMENTO E PAGAMENTO.
- 8.3. Emitir Termos de Aceite, conforme disposto na Cláusula VI – FORNECIMENTO, RECEBIMENTO E ACEITE.

- 8.4. Comunicar à **CONTRATADA** as ocorrências técnicas que demandem assistência técnica, para a adequada abertura de chamada técnica e consequente mobilização do seu pessoal técnico.
- 8.5. Assinar ao término da vigência do presente contrato o Termo de Encerramento e Outras Avenças, conforme modelo Anexo IV deste contrato.

## **IX - PREÇO**

- 9.1. O valor total do presente contrato, fixo e irrevogável, é de R\$ 283.487,54 (duzentos e oitenta e três mil, quatrocentos e oitenta e sete reais e cinquenta e quatro centavos), base janeiro/2024, conforme Anexo II deste contrato.
- 9.2. No valor total estabelecido no item 9.1., estão incluídos todos os tributos, sejam eles federal, estadual ou municipal, sob qualquer título, que incidam ou venham a incidir, direta ou indiretamente sobre este contrato, inclusive, as despesas com seguros, pedágios, viagens, salários, diárias, estadias, alimentação, deslocamento de seus profissionais, encargos sociais de seus profissionais, bem como os serviços de assistência técnica para o reparo dos mesmos, reinstalação em caso de substituição dos **PRODUTOS**, despesas de embalagens, fretes, substituição de todas as peças e componentes que forem avariados durante o período de garantia, todas as documentações, inclusive, manuais do usuário.

## **X - FATURAMENTO E PAGAMENTO**

- 10.1 A **CPTM** procederá ao pagamento nas condições previstas nesta cláusula.
- 10.1.1 Após a aprovação da medição e do recebimento da respectiva Carta de Aprovação de Faturamento - CA, a **CONTRATADA** deverá, no prazo de até 02 (dois) dias úteis, apresentar ao Departamento Fiscal - DFSF da **CPTM**, via endereço eletrônico DFSF-NRDF@cptm.sp.gov.br, o(s) documento(s) fiscal(is) pertinentes à operação, dos quais deverão constar todos os tributos incidentes na fonte sobre a prestação dos serviços, conforme estabelecido na cláusula de tributos deste contrato.
- 10.1.2 No(s) documento(s) fiscal(is) deverá(ão) ser indicados o número do contrato, o período medido, o número da Ordem de Serviço - O.S., o número da medição e os locais de realização dos serviços. No processamento do pagamento, obedecerá a **CPTM** às disposições contidas na Lei nº 8.212, de 24 de julho de 1991, regulamentada pelo Decreto nº 3.048, de 06 de maio de 1999.
- 10.1.3 O documento fiscal não aprovado pela **CPTM** será devolvido à **CONTRATADA** para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo estabelecido no subitem 10.1.1, a partir da data de sua reapresentação.
- 10.1.4 A devolução do documento fiscal não aprovado pela **CPTM** em hipótese alguma servirá de pretexto para que a **CONTRATADA** suspenda a execução dos serviços.

10.1.5 A **CPTM** efetuará o pagamento no prazo de 30 (trinta) dias, a contar da entrega da nota fiscal no DFSF, desde que aprovadas a medição e a nota fiscal, nos prazos estabelecidos nas cláusulas da medição e de pagamento deste contrato.

10.1.5.1 A efetivação do(s) pagamento(s) oriundo(s) deste contrato fica condicionada à inexistência de registro da **CONTRATADA** no CADIN Estadual, nos termos da Lei nº 12.799, de 11 de janeiro de 2008.

10.1.6 Na hipótese de ocorrer devolução da medição, conforme estabelecido na correspondente cláusula deste contrato, o prazo de pagamento será dilatado pelo número de dias contados entre a data de devolução e a(s) data(s) da nova apresentação.

10.1.7 Caso ocorra atraso no pagamento, por motivos imputáveis à **CPTM**, os valores devidos serão acrescidos de juros moratórios de 0,5% (meio por cento) ao mês, calculados “pro rata tempore”, desde a data de vencimento da obrigação até a do efetivo pagamento, conforme fórmula abaixo:

$$VJM = VA \times (1,005)^{n/30}, \text{ onde:}$$

VJM = Valor em atraso acrescido de juros moratórios

VA = Valor em atraso

n = Número de dias em atraso

10.1.8 Excetuam-se os atrasos decorrentes de caso fortuito ou de força maior previstos no artigo 393 do Código Civil Brasileiro, desde que devidamente comprovados.

10.1.9 Os valores de eventuais reajustamentos de preços deverão ser indicados no corpo do documento fiscal e faturados separadamente do valor principal, acompanhados da respectiva memória de cálculo, bem como da cópia da publicação dos índices de preços que compõem a fórmula de reajuste.

10.1.10 Os pagamentos serão efetuados por meio de crédito em conta corrente, junto ao BANCO DO BRASIL S.A., na forma do Decreto 62.867, de 03/10/2017 alterado pelo Decreto Estadual nº 66.000, de 09/09/2021, estando vedada a cobrança bancária.

10.1.11 A **CONTRATADA** deverá informar, por escrito, o tipo, o número da conta corrente, o número e o nome da agência de sua conta, em até 10 (dez) dias úteis contados da data da assinatura do contrato, por correspondência dirigida ao Gestor do contrato.

10.1.12 A **CPTM** poderá, sem prejuízo do disposto na cláusula DAS PENALIDADES, descontar dos pagamentos das faturas importâncias que, a qualquer título, forem-lhe devidas pela **CONTRATADA** em razão do presente contrato ou de qualquer outro celebrado entre a **CPTM** e a **CONTRATADA**.

10.1.13 Quaisquer títulos de cobrança emitidos pela **CONTRATADA** contra a CPTM não poderão ser negociados e deverão ser mantidos em carteira. A **CPTM** não se obriga a efetuar pagamentos de títulos colocados em cobrança por meio de Bancos ou empresas de "factoring".

10.1.14 A **CONTRATADA** dará como quitadas todas as duplicatas ou outros documentos de cobrança sacados contra a **CPTM**, pela efetivação do crédito em sua conta corrente.

## **XI - VIGÊNCIA DO CONTRATO**

11.1. O prazo de vigência do presente contrato é de 90 (noventa) dias, contados a partir da data de sua assinatura.

## **XII - RESCISÃO E PENALIDADES**

12.1. O contrato poderá ser rescindido na forma, com as consequências e pelos motivos previstos no Regulamento de Licitações e Contratos da COMPANHIA PAULISTA DE TRENS METROPOLITANOS – CPTM a partir de 04 de dezembro de 2023, sujeitando-se a **CONTRATADA** à penalidade prevista no artigo 7º da Lei federal nº 10.520/2002 e multas previstas no presente contrato.

12.2. No caso de a **CONTRATADA** estar em situação de recuperação judicial, a convalidação em falência ensejará a imediata rescisão deste contrato, sem prejuízo da aplicação das demais cominações legais.

12.3. No caso de a **CONTRATADA** estar em situação de recuperação extrajudicial, o descumprimento do plano de recuperação ensejará a imediata rescisão deste contrato, sem prejuízo da aplicação das demais cominações legais.

12.4. O presente contrato poderá ser rescindido por quaisquer das partes, pelo não cumprimento de quaisquer condições ou cláusulas estabelecidas neste instrumento, ficando a parte infratora sujeita, a favor da parte inocente, às perdas e danos correspondentes.

12.5. Os casos fortuitos e/ou motivos de força maior serão excludentes da responsabilidade das partes contratantes de acordo com o disposto no artigo 393 do Código Civil Brasileiro.

12.6. Pela inexecução total ou parcial de qualquer cláusula e/ou condição do contrato a **CONTRATANTE** poderá, garantida a prévia defesa, aplicar à **CONTRATADA** as seguintes sanções:

12.6.1. Multa equivalente a 10% (dez por cento) calculada sobre o valor total do contrato, no caso de rescisão, por culpa ou requerimento da **CONTRATADA**, sem motivo justificado ou amparo legal, a critério da **CONTRATANTE**.

12.6.2. Em caso de atraso na entrega dos produtos e/ou na prestação de serviços, conforme previsto neste contrato, a **CONTRATANTE** poderá aplicar multa sobre o valor da obrigação não cumprida, considerando-se os seguintes critérios:



- a) Atraso de até 30 (trinta) dias, multa de 0,3% (zero vírgula três por cento) por dia;
- b) Atraso superior a 30 (trinta) dias, multa de 10% (dez por cento) desconsiderando o previsto no inciso anterior;
- c) Atraso superior a 60 (sessenta) dias, multa de 15% (quinze por cento) do saldo financeiro não realizado, cumulativa com o previsto no inciso b, sem prejuízo das demais sanções administrativas cabíveis.

12.6.3. Em caso de atraso nos prazos de atendimento, relativos à garantia dos **PRODUTOS**, a **CONTRATANTE** poderá aplicar multa sobre o valor do produto que deu causa ao atraso, considerando-se os seguintes critérios:

- a) Atraso de até 24 (vinte e quatro) horas, multa de 0,1% (zero vírgula um por cento) por hora de atraso;
- b) Da 25<sup>a</sup> (vigésima quinta) até a 48<sup>a</sup> (quadragésima oitava) hora de atraso, multa de 0,3% (zero vírgula três por cento) por hora de atraso, cumulada com o previsto no inciso anterior;
- c) Após 48 (quarenta e oito) horas de atraso, a **CONTRATADA** ficará sujeita unicamente à multa de 10% (dez por cento) sobre o valor do produto.

12.6.4. Multa equivalente a 5% (cinco por cento) calculada sobre o valor do faturamento do mês da ocorrência, por infringência de qualquer cláusula, condições ou obrigações pactuadas neste contrato e não abrangidas nas alíneas anteriores. Não havendo faturamento no mês da ocorrência a multa será de 0,4% (zero vírgula quatro por cento) sobre o valor total do contrato.

12.6.4.1. Em caso de reincidência do descumprimento contratual, a multa estabelecida terá seu percentual acrescido em 50% (cinquenta por cento).

12.6.5. Impedimento para licitar e contratar com a Administração Estadual, de acordo com o artigo 7º da Lei federal nº 10.520/2002 e Súmula nº 51 do Tribunal de Contas do Estado de São Paulo.

12.7. Ficará a critério da **CONTRATANTE** a aplicação cumulativa ou não das sanções acima.

12.8. As penalidades serão aplicadas sem prejuízo das multas previstas no ato convocatório, após ter sido garantido o exercício do direito de defesa e registradas no Cadastro Unificado de Fornecedores do Estado de São Paulo - CAUFESP.

12.9. As multas previstas neste contrato poderão ser descontadas dos pagamentos devidos ou cobrados da **CONTRATADA**, através de cobrança direta e autônoma, pela via administrativa ou judicial.

12.10. No caso de não existirem pagamentos pendentes, a **CONTRATADA** deverá efetuar a quitação da multa em até 48 (quarenta e oito) horas contadas do recebimento do documento de cobrança respectivo, por meio de depósito bancário, sob pena de, em não o fazendo, sujeitar-se aos procedimentos judiciais cabíveis.

12.11. Os valores referentes às multas, indenizações e demais importâncias quando não ressarcidos pela **CONTRATADA**, serão atualizados pelo IPC-FIPE, calculado pro rata dia e acrescido de juros de mora de 12% (doze por cento) ao ano.

12.12. Sem prejuízo da aplicação de penalidades, a **CONTRATADA** é responsável pelos danos causados à **CONTRATANTE** ou a terceiros, na forma disposta no artigo 76 da Lei federal nº 13.303/2016, ou outras disposições legais, se aplicável, não excluindo ou reduzindo essa responsabilidade, a fiscalização ou acompanhamento pelo órgão interessado.

12.13. As partes poderão rescindir o presente contrato mediante acordo.

### **XIII - DISPOSIÇÕES FINAIS**

13.1. O presente contrato é regido pelas suas cláusulas, pelo disposto na Lei federal nº 13.303/2016, se aplicável, pela Lei federal nº 10.520/2002, pelo Decreto Estadual nº 63.722/2018, Decreto Estadual nº 47.297, de 06 de novembro de 2002, do Decreto Estadual nº 49.722, de 24 de junho de 2005, pela Norma Implementadora nº 03/002, do Regulamento de Licitações e Contratos da Companhia Paulista de Trens Metropolitanos – CPTM, vigente a partir de 04 de dezembro de 2023, pela Lei Complementar nº 123, de 14 de dezembro de 2006, as disposições do Capítulo II-B do Título XI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), do Código de Conduta e Integridade e Código de Conduta e Integridade de Fornecedores, Prestadores de Serviços e Parceiros da CPTM, pela Lei Federal nº 13.709, de 14 de agosto de 2018, com suas alterações subsequentes, bem como toda a legislação aplicável sobre privacidade e proteção de dados, inclusive, normas setoriais ou gerais sobre o tema, e pelas demais normas regulamentares aplicáveis à espécie e pelos preceitos de direito privado.

13.2. O presente contrato, a execução de seu objeto, produtos e/ou serviços não poderão ser cedidos ou transferidos total ou parcialmente pela **CONTRATADA**, a terceiros estranhos a esta contratação.

13.3. A **CONTRATADA**, mediante acordo, poderá anuir na cessão ou transferência total ou parcial deste contrato da **CONTRATANTE** para qualquer de seus clientes e/ou entes em geral, mantidas as condições nele estabelecidas.

13.4. O cumprimento, durante a execução dos serviços, das leis federais, estaduais e municipais vigentes, correrão por conta da **CONTRATADA**, única e exclusiva responsável pelas infrações que houver.

13.5. Qualquer omissão ou tolerância das partes no exigir o estrito cumprimento das cláusulas e condições deste contrato ou no exercer uma prerrogativa dele decorrente, não constituirá renúncia e nem afetará o direito da parte contratante em exercê-lo a qualquer tempo.

- 13.6. As relações entre a **CONTRATADA** e a **CONTRATANTE**, serão sempre por escrito, ressalvados os entendimentos verbais motivados pela urgência dos serviços, que, entretanto, deverão ser, com a maior brevidade, confirmados por escrito.
- 13.7. As cláusulas deste contrato prevalecerão sempre em relação a qualquer acordo verbal ou escrito, ajustado anterior ou posteriormente à data de sua assinatura, bem como em relação às disposições eventualmente conflitantes com o edital da licitação que o originou, a menos que sejam expressamente revogadas pelas partes, através de termo de retificação a este contrato.
- 13.8. O disposto neste contrato não poderá ser alterado ou emendado pelas partes, salvo por meio de Termo Aditivo.
- 13.9. A **CONTRATADA** ficará sujeita à instauração de processo administrativo de responsabilização, nos termos da Lei federal nº 12.846/2013 e do Decreto estadual nº 67.301/2022, sem prejuízo das sanções administrativas previstas nos artigos 83 e 84 da Lei federal nº 13.303/2016, ou outras disposições legais, se aplicável, caso incorra na prática de atos que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou que de qualquer forma venham a construir fraude ou corrupção ao longo da execução deste contrato.

#### **XIV – ANEXOS**

- 14.1. Integram o presente contrato os seguintes anexos:

Anexo I - Termo de Referência - (Anexo I do Edital);

Anexo II - Descrição dos Produtos e/ou Serviços;

Anexo III - Termo de Ciência e de Notificação - Tribunal de Contas do Estado de São Paulo;

Anexo IV - Termo de Encerramento e Outras Avenças – Modelo.

#### **XV - FORO**

15.1. As partes contratantes elegem como foro competente o da comarca de São Paulo, estado de São Paulo, com renúncia de qualquer outro por mais privilegiado que seja para dirimir as questões porventura decorrentes da execução deste contrato.

E, por estarem assim justas e contratadas, as Partes e testemunhas firmam o presente instrumento.

**Pela COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM:**

ANA CAROLINE DE FARIA EDUARDO BORGES

Diretora Administrativa e Financeira

ana.borges@cptm.sp.gov.br

E-mail pessoal: N/I

CPF Nº 003.938.371-73

RG Nº 429674-9



Documento assinado digitalmente

ANA CAROLINE DE FARIA EDUARDO BORGES

Data: 27/12/2024 17:48:27-0300

Verifique em <https://validar.iti.gov.br>



MICHAEL SOTELO CERQUEIRA  
Diretor Presidente  
michael.cerqueira@cptm.sp.gov.br  
E-mail pessoal: N/I  
CPF Nº 284.295.458-08  
RG Nº 33.427.569-6



Documento assinado digitalmente  
MICHAEL SOTELO CERQUEIRA  
Data: 27/12/2024 19:16:26-0300  
Verifique em <https://validar.iti.gov.br>

JOSÉ LUIZ BARCI NEVES  
Gerente de Tecnologia da Informação  
jose.barci@cptm.sp.gov.br  
E-mail pessoal: N/I  
CPF Nº 853.555.507-20  
RG Nº 39.326.561-4



Documento assinado digitalmente  
JOSE LUIZ BARCI NEVES  
Data: 27/12/2024 17:14:29-0300  
Verifique em <https://validar.iti.gov.br>

### Pela CONTRATADA:

NEIVA MARIA DA SILVA  
Procuradora  
neiva.silva@ingrammicro.com  
E-mail pessoal: N/I  
CPF nº 157.847.158-36  
RG nº 24.476.027-5

NEIVA MARIA DA SILVA:15784715836  
Assinado de forma digital por  
NEIVA MARIA DA  
SILVA:15784715836  
Dados: 2024.12.27 16:29:17  
-03'00'

FRANCISCO AUGUSTO ZANET  
Procurador  
francisco.zanet@ingrammicro.com  
E-mail pessoal: N/I  
CPF nº 010.602.688-76  
RG nº 9.447.462-x

FRANCISCO AUGUSTO ZANET:0106026887668876  
Assinado de forma digital por FRANCISCO AUGUSTO ZANET:01060268876  
Dados: 2024.12.27 16:53:30 -03'00'

### TESTEMUNHAS:

ALEXANDRE FRANCISCO  
Assistente Administrativo



Documento assinado digitalmente  
ALEXANDRE FRANCISCO  
Data: 27/12/2024 16:10:57-0300  
Verifique em <https://validar.iti.gov.br>

EDUARDO DA SILVA PRADO  
Assistente Administrativo



Documento assinado digitalmente  
EDUARDO DA SILVA PRADO  
Data: 27/12/2024 17:27:03-0300  
Verifique em <https://validar.iti.gov.br>

## **ANEXO I**

### **Termo de Referência - (Anexo I do Edital)**

## **ANEXO I**

### **TERMO DE REFERÊNCIA REL.GEX.007/2023 v.1.1**

#### **ANEXO I-A**

### **DECLARAÇÃO DE PRODUTOS A SEREM FORNECIDOS**





Governo do Estado de São Paulo  
Companhia de Processamento de Dados do Estado de São Paulo  
Gerência Executiva

## TERMO DE REFERÊNCIA

**Nº do Processo:** 359.00001160/2023-10

**Interessado:** Gerência de Segurança da Informação

**Assunto:** Ata de Registro de Preços - Equipamentos de Firewall

## TERMO DE REFERÊNCIA REL.GEX.007/2023 v.1.1

### TERMO DE REFERÊNCIA

**CONTRATAÇÃO FUTURA DE SOLUÇÃO DE PROTEÇÃO DE REDES NGFW – NEXT GENERATION  
FIREWALL ATRAVÉS DO SISTEMA DE REGISTRO DE PREÇOS PARA A PRODESP E ÓRGÃOS  
PARTICIPANTES**

REL.GEX.007/2023 v.1.1

setembro/2023

TERMO DE REFERÊNCIA: fornece as especificações técnicas mínimas necessárias as quais o produto e/ou serviço ofertado pela proponente deverá obrigatoriamente atender.

## PREÂMBULO

### CONTEÚDO DO ANEXO I

**ANEXO I – TERMO DE REFERÊNCIA:** fornece as especificações técnicas mínimas necessárias às quais o produto ou serviço ofertado pela proponente deverá obrigatoriamente atender.

**ANEXO I-A – DECLARAÇÃO DE PRODUTOS A SEREM FORNECIDOS:** o Anexo I-A deverá ser entregue assinado pelo representante legal, conforme disposto no Contrato Social ou Estatuto, com carimbo ou identificação da assinatura, utilizando preferencialmente este Anexo. Qualquer observação de âmbito técnico deverá ser feita apenas no Anexo I-A.

**ANEXO I-B – RELAÇÃO DE ÓRGÃOS PARTICIPANTES:** fornece a relação de todos os órgãos participantes da Ata de Registro de Preços, bem como distribuição da quantidade de cada item por Órgão.

**ANEXO I-C – LOCAIS DE ENTREGA:** fornece os locais de entrega de cada órgão participante

1. **OBJETO**

1.1. Contratação de empresa especializada em tecnologia da informação para fornecimento de solução de proteção de redes com característica de “**Next Generation Firewall – NGFW**”, com serviços de instalação, configuração, treinamento e garantia on-site de 60 meses.

2. **ITENS A SEREM OFERTADOS**

2.1. **SOLUÇÃO DE FIREWALL TIPOS 1, 2, 3, 4, 5 e 6**

ITEM	DESCRIÇÃO
1	Firewall TAMANHO DATACENTER – Tipo 1 - HardwareFirewall TAMANHO DATACENTER – Tipo 1 - Softwares / Licenças / Subscrições / Assinaturas
2	Firewall TAMANHO GRANDE - Tipo 2 – HardwareFirewall TAMANHO GRANDE - Tipo 2 - Softwares / Licenças / Subscrições / Assinaturas
3	Firewall TAMANHO MÉDIO1 – Tipo 3 – HardwareFirewall TAMANHO MÉDIO1 – Tipo 3 - Softwares / Licenças / Subscrições / Assinaturas
4	Firewall TAMANHO MÉDIO2 – Tipo 4 – HardwareFirewall TAMANHO MÉDIO2 – Tipo 4 - Softwares / Licenças / Subscrições / Assinaturas
5	Firewall TAMANHO PEQUENO1 – Tipo 5 – HardwareFirewall TAMANHO PEQUENO1 – Tipo 5 – Softwares / Licenças / Subscrições / Assinaturas
6	Firewall TAMANHO PEQUENO2 – Tipo 6 – HardwareFirewall TAMANHO PEQUENO2 – Tipo 6 – Softwares / Licenças / Subscrições / Assinaturas
7	Módulo Transceptor QSFP28, 100GE, para fibra óptica multimodo, de curto alcance
8	Módulo Transceptor QSFP+, 40GE, para fibra óptica multimodo, de curto alcance
9	Módulo Transceptor SFP28, 25GE, para fibra óptica multimodo, de curto alcance
10	Módulo Transceptor SFP+, 10GE, para fibra óptica multimodo
11	Módulo Transceptor SFP, 1GE, para óptica multimodo
12	Cordão óptico MM 50/125 OM4 LC duplex LSZH
13	Solução de Gerência Centralizada de Firewall – <b>GCFRH1</b> , Hardware para gerenciar no mínimo 25 Firewalls, incluindo software, licenças, subscrições e assinaturas necessárias.
14	Solução de Gerência Centralizada de Firewall – <b>GCFRH2</b> , Hardware para gerenciar no mínimo 150 Firewalls, incluindo software, licenças, subscrições e assinaturas necessárias.
15	Solução de Gerência Centralizada de Firewall – <b>GCFRH3</b> , Hardware para gerenciar no mínimo 1.000 Firewalls, incluindo software, licenças, subscrições e assinaturas necessárias.
16	Solução de Gerência Centralizada de Firewalls – <b>GCVA</b> , Appliance Virtual licenciado e com capacidade para gerenciar no mínimo 10 Firewalls, para utilização em infraestrutura de Máquina Virtual já existente.
17	Pacote de licenças <b>GCVAEXP1</b> para no mínimo 10 firewalls adicionais e todas as demais licenças, suporte e subscrições, que forem necessárias para expansão da capacidade da Gerência Centralizada de Firewall, <b>GCVA</b> .
18	Pacote de licenças <b>GCVAEXP2</b> para no mínimo 50 firewalls adicionais e todas as demais licenças, suporte e subscrições, que forem necessárias para expansão da

	capacidade da Gerência Centralizada de Firewall, <b>GCVA</b> .
19	Pacote de licenças <b>GCVAEXP3</b> para no mínimo 100 firewalls adicionais e todas as demais licenças, suporte e subscrições, que forem necessárias para expansão da capacidade da Gerência Centralizada de Firewall, <b>GCVA</b> .
20	Solução de Gerência de Relatórios, Logs e Incidentes – <b>GCRLIH1</b> , Hardware para gerenciar no mínimo 25GB Logs por dia, incluindo software, licenças, subscrições e assinaturas necessárias.
21	Solução de Gerência de Relatórios, Logs e Incidentes – <b>GCRLIH2</b> , Hardware para gerenciar no mínimo 100GB Logs por dia, incluindo software, licenças, subscrições e assinaturas necessárias.
22	Solução de Gerência de Relatórios, Logs e Incidentes – <b>GCRLIH3</b> , Hardware para gerenciar no mínimo 600GB Logs por dia, incluindo software, licenças, subscrições e assinaturas necessárias.
23	Solução de Gerência de Relatórios, Logs e Incidentes – <b>GCRLIVA</b> - Appliance Virtual licenciado e com capacidade para gerenciar no mínimo 25 GB Logs por dia.
24	Pacote de licenças <b>GCRLIVAEXPL1</b> para no mínimo 5 GB de logs por dia adicionais e todas as demais licenças, suporte e subscrições, que forem necessárias para expansão da capacidade da Solução de Gerência de Relatórios, Logs e Incidentes – <b>GCRLIVA</b> ,
25	Pacote de licenças <b>GCRLIVAEXPL2</b> para no mínimo 25 GB de logs por dia adicionais e todas as demais licenças, suporte e subscrições, que forem necessárias para expansão da capacidade da Solução de Gerência de Relatórios, Logs e Incidentes – <b>GCRLIVA</b> ,
26	Pacote de licenças <b>GCRLIVAEXPL3</b> para no mínimo 100 GB de logs por dia adicionais e todas as demais licenças, suporte e subscrições, que forem necessárias para expansão da capacidade da Solução de Gerência de Relatórios, Logs e Incidentes – <b>GCRLIVA</b> ,
27	Instalação do FIREWALL Tipo 1 - Região Metropolitana de São Paulo
28	Instalação do FIREWALL Tipo 1 - Interior de São Paulo
29	Instalação do FIREWALL Tipo 2 - Região Metropolitana de São Paulo
30	Instalação do FIREWALL Tipo 2 – Interior de São Paulo
31	Instalação do FIREWALL Tipo 3 - Região Metropolitana de São Paulo
32	Instalação do FIREWALL Tipo 3 – Interior de São Paulo
33	Instalação do FIREWALL Tipo 4 - Região Metropolitana de São Paulo
34	Instalação do FIREWALL Tipo 4 – Interior de São Paulo
35	Instalação do FIREWALL Tipos 5 - Região Metropolitana de São Paulo
36	Instalação do FIREWALL Tipos 5 – Interior de São Paulo
37	Instalação do FIREWALL Tipos 6 - Região Metropolitana de São Paulo
38	Instalação do FIREWALL Tipos 6 – Interior de São Paulo
39	Instalação da Gerência Centralizada de FIREWALL - Região Metropolitana de São Paulo
40	Instalação da Gerência Centralizada de FIREWALL – Interior
41	Instalação da Gerência Relatórios, Logs e Incidentes - Região Metropolitana de São Paulo
42	Instalação da Gerência Relatórios, Logs e Incidentes – Interior
43	Treinamento da Solução de FIREWALL
44	Treinamento da Solução de Gerência Centralizada para FIREWALL

### 3. CARACTERÍSTICAS COMUNS A TODOS FIREWALLS

#### 3.1. CONDIÇÃO GERAL

3.1.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante será

empregado como NGFW ou simplesmente FIREWALL;

3.1.2. Todos os modelos de Tipos de Firewalls ofertados, devem ser do mesmo fabricante e compatíveis com os todos itens de gerência centralizada e gerência de relatórios e logs;

3.1.3. O equipamento deverá ser novo e sem uso anterior. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada;

3.1.4. Todos os equipamentos devem ser novos e sem uso anterior;

3.1.5. O fabricante deve publicar as vulnerabilidades conhecidas em cada versão das plataformas NGFW e Gerenciamento, detalhar o meio de os meios de correções diante de um relatório PSIRT;

3.1.6. Por funcionalidades de Firewall entende-se: um firewall com inspeção de estado (stateful) que permita ou bloqueia tráfego de acordo com o estado, a porta e o protocolo;

3.1.7. Por funcionalidades de NGFW entende-se: firewall, controle de aplicações, prevenção de ameaças e IPS (intrusion prevention system). Esta taxa deve referenciar-se a tráfego multiprotocolo em ambiente de produção, tráfego considerado de mundo real ou tráfego misto, ou seja, aquele que não faz referência apenas a um protocolo e/ou um tamanho de pacote para teste em condição ideal;

3.1.8. Por funcionalidades de Threat Prevention entende-se as seguintes funcionalidades habilitadas simultaneamente: Controle de aplicação, IPS (Intrusion Prevention System), Antimalware. Esta taxa deve referenciar-se a tráfego multiprotocolo em ambiente de produção, tráfego considerado de mundo real ou tráfego misto, ou seja, aquele que não faz referência apenas a um protocolo e/ou um tamanho de pacote para teste em condição ideal;

3.1.9. Para proteção do ambiente contra ataques cibernéticos, o dispositivo de proteção deve possuir módulo de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados no próprio appliance de NGFW;

3.1.10. Deve implementar em um único dispositivo, de forma integrada, tecnologia de Next Generation Firewall com capacidade para filtro de pacotes, controle de aplicação, VPN IPsec e SSL, IPS, prevenção contra ameaça de vírus, spywares e malwares e filtro de conteúdo/URL, além de haver integração com sandbox para prevenção contra ameaças avançadas;

3.1.11. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

3.1.12. Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço;

3.1.13. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes;

3.1.14. Todos os equipamentos appliances do tipo firewall ofertados, devem possuir homologação da ANATEL, emitida e válida no dia do certame/pregão.

## 3.2. CARACTERÍSTICAS TÉCNICAS

### 3.2.1. CARACTERÍSTICAS DIVERSAS

3.2.1.1. Deve implementar o controle do tráfego para os protocolos TCP, UDP, ICMP e aplicações/serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino;

3.2.1.2. Suportar inspeção stateful de tráfego IPv4 e IPv6;

3.2.1.3. Suportar a criação de regras IPv4 e IPv6;

3.2.1.4. Deverá suportar dual stack IPv4/IPv6, ICMPv6, DNSv6;

3.2.1.5. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPsec;

- 3.2.1.6. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 3.2.1.7. Deve suportar NAT64 e NAT46;
- 3.2.1.8. Possuir funcionalidade de DHCP Relay e DHCP Server;
- 3.2.1.9. Deve possuir suporte a roteamento multicast (PIM-SM e PIM-DM) e IGMP V2 e V3;
- 3.2.1.10. Deve possuir proteção anti-spoofing;
- 3.2.1.11. Deve suportar OSPF graceful restart ou OSPF ECMP;
- 3.2.1.12. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 3.2.1.13. Suportar a funcionalidade de proxy chaining, possibilitando a integração com ferramentas de terceiros para ao menos a funcionalidade de DLP, através de protocolo ICAP;
- 3.2.1.14. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 3.2.1.15. Possuir servidor de DHCP (dynamic host configuration protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e em VPN;
- 3.2.1.16. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de aplicações em horários específicos;
- 3.2.1.17. Deve permitir a utilização de regras de antivírus, antispymware, IPS e filtro de conteúdo web por segmentos de rede. Todas as aplicações devem ser suportadas no mesmo segmento de rede ou VLAN;
- 3.2.1.18. Deve contemplar VIRTUAL patching com integração nativa na rede de inteligência cibernética do Fabricante com intuito de auto proteger as vulnerabilidades apresentadas pelo relatório PSIRT, descrito no item 3.1.5, podendo ser atendido mediante licenciamento da funcionalidade de IPS;
- 3.2.1.19. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
- 3.2.1.20. A inspeção SSL deve ser compatível com HTTP/3. Tal inspeção é essencial uma vez que uma grande quantidade de sítios públicos está utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos;
- 3.2.1.21. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares por meio do Microsoft TEAMS para usuários da rede, individualmente ou em grupo;
- 3.2.1.22. Deve ter suporte à proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas gerar registro e identificar as máquinas possivelmente contaminadas e ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, como também ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso;
- 3.2.1.23. Possuir assinaturas específicas ou implementar mecanismo interno no appliance para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciado;
- 3.2.1.24. Ser capaz de bloquear ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- 3.2.1.25. Detectar e bloquear a origem de portscans;
- 3.2.1.26. Deve permitir o bloqueio de ataques;
- 3.2.1.27. Deve permitir o bloqueio de exploits conhecidos;
- 3.2.1.28. A solução de firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, hashes de malwares e domínios;

- 3.2.1.29. O gateway antivírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP e SMTP;
- 3.2.1.30. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL onde o mesmo deverá ser descriptografado de forma transparente à aplicação;
- 3.2.1.31. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP e SIP, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora, quanto, de fora para dentro;
- 3.2.1.32. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 3.2.1.33. Implementar controle e gerenciamento de banda para a tecnologia VoIP (Voice over Internet Protocol) sobre diferentes segmentos de rede/segurança com inspeção profunda de segurança sobre este serviço;
- 3.2.1.34. Implementar mecanismo de sincronismo de horário através do protocolo NTP;
- 3.2.1.35. Possuir suporte ao protocolo SNMP versões 2 e 3;
- 3.2.1.36. Possui suporte a log via syslog;
- 3.2.1.37. Possuir suporte aos protocolos de roteamento RIP, RIPv2, RIPng, BGP, OSPF, OSPFv2 e OSPFv3. As configurações dos protocolos elencados, devem ser feitos através da interface gráfica;
- 3.2.1.38. Para BGP, deve suportar o anúncio condicional de communities em função de health checks efetuados pela solução;
- 3.2.1.39. Reconhecer aplicações como no mínimo peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail e aplicações SaaS;
- 3.2.1.40. Deve suportar ao menos 128 tabelas independentes de roteamento, por contexto de firewall;
- 3.2.1.41. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 3.2.1.42. Permitir a criação de assinaturas customizadas de acordo com o fluxo de acesso dos usuários a serviços internos;
- 3.2.1.43. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) ou Saída (Outbound);
- 3.2.1.44. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
- 3.2.1.45. Deve suportar VLAN Tags padrão 802.1q, adicionalmente agregação de portas utilizando protocolo 802.3ad, com algoritmo de balanceamento L2, L3 e L4;
- 3.2.1.46. A solução de firewall deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
- 3.2.1.47. Para agilizar a gerência remota do firewall, deve ser possível carregar conteúdo estático dela a partir de objetos em cache em CDNs;
- 3.2.1.48. A solução de firewall deve efetuar restrição de TENANT para os provedores de SaaS Microsoft e Google, permitindo a manipulação de cabeçalhos HTTP ou HTTPS, visando incluir informações requeridas pelo provedor de serviço SaaS, garantindo acesso aos serviços apenas para e-mails e aplicativos do domínio cadastrado;
- 3.2.1.49. Todos os equipamentos fornecidos do tipo Firewall devem ser próprios para montagem em rack 19", com altura máxima de 02 RUs (duas unidades de altura de rack), exceto para tipos 5 e 6, estes



podendo ser entregues em formato de Desktop;

3.2.1.50. A solução ofertada deve continuar operando de forma nativa e totalmente automática, sem qualquer tipo de intervenção manual, mantendo as funcionalidades de controle de aplicação, antivírus e IPS, ainda que não permaneça o direito de atualização de suas bases de assinaturas, vacinas e uso de sandbox em nuvem, bem como categorização dinâmica de sites, uma vez expirado o licenciamento;

3.2.1.51. Deve possuir integração com soluções de NAC, para autenticação SSO no firewall de elementos registrados no NAC e execução de políticas de compliance na VPN;

3.2.1.52. Devem incluir 2 (dois) tokens mobile, por NGFW, sem custo, permitindo o uso de múltiplo fator de autenticação na gerência dos firewalls. Esse item pode ser entregue em composição com solução de fabricante diferente do Firewall;

### 3.2.2. CARACTERÍSTICAS DE VPN

3.2.2.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e aplicações. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC

3.2.2.2. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, Certificados digitais e XAUTH client authentication

3.2.2.3. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário

3.2.2.4. Suportar encapsulamento de VRFs através dos tuneis IPSec, permitindo a segmentação lógica de redes em todo o ambiente WAN, de acordo com a escalabilidade descrita no item 3.2.1.40.

### 3.2.3. CONTROLE DE AMEAÇAS

3.2.3.1. Deve implementar mecanismos de proteção de “dia zero” (Zero Day Protection), isto é, para ameaças que não possuam assinaturas. Para este tipo de proteção, a solução de segurança deverá reter eventual ameaça, uma vez identificada. A análise desta ameaça deve ser realizada em ambiente de nuvem do próprio fabricante da solução. Será também aceito appliance físico ou virtual (nesse último caso, considerando o provimento de todo o hardware necessário para suportar o recurso), a ser instalado no ambiente da CONTRATANTE, sendo necessário estar licenciado para atendimento das duas situações (nuvem e ambiente da CONTRATANTE), inclusive licenças de sistema operacional para emulação dos artefatos.”;

3.2.3.2. Para as ameaças de dia zero, a solução deve ter a habilidade de prevenir o ataque;

### 3.2.4. CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB E FILTRO DE DNS

3.2.4.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 80 (oitenta) categorias distintas, com mecanismo de atualização automática;

3.2.4.2. Deve bloquear requisições de domínios conhecidos como “Command and Control” de botnets;

3.2.4.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

3.2.4.4. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet,

sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico;

3.2.4.5. Permitir a customização de página de bloqueio;

3.2.4.6. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante;

3.2.4.7. Deve possuir funcionalidade para forçar o uso de Safe Search para, ao menos, os buscadores do Google, Bing e Youtube;

3.2.4.8. Ter a capacidade de permitir ou bloquear novos domínios criados a fim de evitar campanha de malwares;

3.2.4.9. Deve permitir submissão de novos sites para categorizar;

3.2.4.10. Permitir a classificação dinâmica de sites web, URLs e domínios, com o veredicto em tempo real, com a rede de inteligência do fabricante;

3.2.4.11. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;

3.2.4.12. Permitir regra, com controle de autenticação, filtrando através de grupos de usuários importados de fontes externas, possibilitando único login SSO originados dos serviços Active Directory, TS e Citrix.

3.2.4.13. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

3.2.4.14. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web;

3.2.4.15. Permitir a inspeção de acesso a sites criptografados, observando o SNI dos domínios, sem a necessidade de interceptar o tráfego via decifração SSL;

3.2.4.16. Permitir a exceções de Sites confidenciais de categorias ao menos, saúde e financeiros, na interceptação do tráfego via decifração SSL;

3.2.4.17. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia e dia da semana;

### 3.2.5. CARACTERÍSTICAS DE AUTENTICAÇÃO

3.2.5.1. Prover autenticação de usuários para os serviços/aplicações Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea;

3.2.5.2. Permitir a autenticação dos usuários utilizando servidores LDAP e AD;

3.2.5.3. Possuir integração com servidores de autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;

3.2.5.4. Permitir autenticação e login único "SSO" em plataformas Terminal Server e Citrix;

3.2.5.5. Deve suportar SAML como método para autenticação na navegação de Internet e para VPN;

3.2.5.6. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento;

3.2.5.7. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW;

3.2.5.8. Permitir o controle por usuário de plataformas Microsoft Windows 7, Windows 8 e Windows 10, em modo transparente, para todas as aplicações suportadas, de forma que ao efetuar o

logon na rede, um determinado usuário só consiga acessar as aplicações permitidas pelo seu perfil, sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser;

3.2.5.9. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW ou externo;

3.2.5.10. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando;

3.2.5.11. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

### 3.2.6. CARACTERÍSTICAS DE ADMINISTRAÇÃO

3.2.6.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração;

3.2.6.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW;

3.2.6.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração;

3.2.6.4. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões;

3.2.6.5. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real;

3.2.6.6. Permitir a visualização, em tempo real, das aplicações com maior tráfego e os endereços IPs mais acessados;

3.2.6.7. Deve suportar no mínimo dois tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário (discard), Drop com notificação do bloqueio ao usuário (drop), Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

### 3.2.7. CONTROLE E BALANCEAMENTO INTELIGENTE DE APLICAÇÕES

3.2.7.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

3.2.7.2. Deve ser possível criar políticas que definam os seguintes critérios para match:

3.2.7.3. Endereços de origem;

3.2.7.4. Grupos de usuários;

3.2.7.5. Endereços de destino;

3.2.7.6. DSCP;

3.2.7.7. Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

3.2.7.8. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

3.2.7.9. Deverá balancear o tráfego das aplicações entre, pelo menos, 5 (cinco) links simultaneamente, inclusive 4G/5G e MPLS IntraGOV;

- 3.2.7.10. O firewall deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo (sessão) entre múltiplos links simultaneamente;
- 3.2.7.11. Deve possuir suporte ao MOS (Mean Opinion Score), para calcular a qualidade de chamadas de voz, considerando jitter, perda de pacote e codec utilizado;
- 3.2.7.12. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;
- 3.2.7.13. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 3.2.7.14. A solução deve permitir a definição do roteamento para cada aplicação;
- 3.2.7.15. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;
- 3.2.7.16. Deve possibilitar a definição do link de saída para uma aplicação específica;
- 3.2.7.17. Deve implementar balanceamento de link por hash do IP de origem;
- 3.2.7.18. Deve implementar balanceamento de link por hash do IP de origem e destino;
- 3.2.7.19. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
- 3.2.7.20. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- 3.2.7.21. A solução deve possuir suporte a Policy based routing ou policy based forwarding;
- 3.2.7.22. Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);
- 3.2.7.23. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 3.2.7.24. Deve ser possível habilitar o FEC para tráfegos específicos. Ex: apenas para aplicações sensíveis a perda de pacote;
- 3.2.7.25. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;
- 3.2.7.26. A solução deve suportar nativamente conectores com clouds públicas. Pelo menos: Azure, AWS e GCP;
- 3.2.7.27. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:
- 3.2.7.28. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;
- 3.2.7.29. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- 3.2.7.30. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;
- 3.2.7.31. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;
- 3.2.7.32. O QoS deve possibilitar a definição de fila de prioridade;

- 3.2.7.33. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;
- 3.2.7.34. A capacidade de agendar intervalos de tempo em que as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;
- 3.2.7.35. Deve possibilitar a definição de bandas distintas para download e upload;
- 3.2.7.36. A solução deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);
- 3.2.7.37. A solução deve suportar health check ativo, passivo e misto:
- 3.2.7.38. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 3.2.7.39. Passivo: uso do tráfego real para as medições;
- 3.2.7.40. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo;
- 3.2.7.41. A funcionalidade de controle e balanceamento inteligente de aplicações deve suportar IPv6;
- 3.2.7.42. Deve ser capaz de bloquear acesso às aplicações;
- 3.2.7.43. Deve suportar NAT dinâmico bem como NAT de saída;
- 3.2.7.44. Deve suportar balanceamento de tráfego por sessão e pacote;

### 3.2.8. FILTRO DE DADOS

- 3.2.8.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
- 3.2.8.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 3.2.8.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 3.2.8.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

### 3.2.9. VPN CLIENT-SSL

- 3.2.9.1. Cada firewall deve suportar, no mínimo, a quantidade de Conexões VPN-SSL referentes ao Tipo de Firewall, especificados no item **5. REQUISITOS MÍNIMOS - FIREWALL**, presente nesse termo. Caso seja um recurso licenciado, deve ser entregue em sua capacidade máxima, além do mínimo requisitado;
- 3.2.9.2. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento e por meio de portal web;
- 3.2.9.3. Deverá possuir VPN SSL e deverá manter uma conexão segura com o portal durante a sessão;
- 3.2.9.4. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 3.2.9.5. Deve ser possível realizar, no mínimo, as seguintes verificações da estação do usuário durante a conexão de VPN: sistema operacional, antivírus habilitado e firewall habilitado;

3.2.9.6. O agente de VPN SSL client-to-site, o qual deve ser do mesmo fabricante do Firewall, deve ser compatível com pelo menos: Windows 8.1 (32 e 64 bit), Windows 10 (32 e 64 bit), Windows 11 (64 bit), Mac OS X (v10.15 ou superior), Android (versão 12 ou superior) e Apple iOS (versão 15 ou superior);

### 3.2.10. ESCALABILIDADE E ALTA DISPONIBILIDADE

3.2.10.1. Cada unidade de firewall deve permitir e estar licenciada para utilização em Alta Disponibilidade com outra unidade do mesmo modelo;

3.2.10.2. Deverá centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

3.2.10.3. Deverá permitir que as políticas sejam aplicadas automaticamente a todos os membros do cluster, de modo que o administrador não precise definir configurações separadas para cada unidade firewall do cluster;

3.2.10.4. O sincronismo dos servidores deve ser por interface de sincronização ou por interface de dados;

3.2.10.5. O cluster não deverá derrubar as conexões existentes quando for aplicada uma nova política de segurança;

3.2.10.6. Deverão ser estruturados em cluster, de forma redundante, permitindo failover completo na ocorrência de falhas, suportando modo de operação ativo/ativo e ativo/passivo sem a necessidade de licenças adicionais;

3.2.10.7. Os equipamentos devem ser entregues em configuração de alta disponibilidade e com todas as licenças necessárias para a configuração em modo ativo/ativo;

3.2.10.8. Deverá possuir mecanismos de teste de link com o objetivo de fazer com que appliances do cluster fiquem offline se houver falha de link associado aquele appliance;

3.2.10.9. O cluster deverá suportar failover de tráfego quando operando em modo ativo-ativo e ativo/passivo;

3.2.10.10. O cluster deverá compartilhar todas as tabelas de estado das conexões, incluindo conexões autenticadas e de VPN, bem como o estado operacional de cada um dos componentes do cluster;

3.2.10.11. Deve permitir o sincronismo de sessões entre diferentes cluster, geograficamente separados, com a mesma similaridade de serviços, garantindo que, em caso de falha em um Data Center, o segundo cluster preserve as sessões ativas stateful;

### 3.2.11. ACESSÓRIOS E LITERATURAS TÉCNICAS (PARA CADA EQUIPAMENTO)

3.2.11.1. Cabo para fonte de alimentação de energia elétrica, padrão ABNT 14136 (2P+T);

3.2.11.2. Conjunto (kit) para montagem em rack de 19 polegadas, exceto para firewalls tipo 5 e 6;

3.2.11.3. Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, documentação técnica e manuais (podendo ser em CD-ROM, DVD ou via portal web) que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

## 4. CARACTERÍSTICAS DE GERÊNCIAS

### 4.1. GERÊNCIAS CENTRALIZADAS DE FIREWALL

#### 4.1.1. FUNCIONALIDADES



- Deve ser uma solução capaz de gerenciar todo e qualquer Tipo de FIREWALL ofertados para esse edital, especificados neste anexo no item 5. REQUISITOS MÍNIMOS – FIREWALL;
- O software de gerenciamento centralizado dos NGFW deve possibilitar:
- A configuração, operação e manutenção (troubleshooting) dos elementos de segurança via interface de gerência;
- Classificação dos elementos de segurança em grupos e, então, aplicar políticas de segurança específicas ao grupo, sendo que a distribuição destas políticas é feita de forma automática pelo sistema de gerenciamento. O sistema também deve permitir a criação e aplicação de regras globais de segurança;
- Deve suportar, sem custo adicional, a virtualização da gerência, segregando a gestão dos firewalls em contextos distintos. Deve suportar, pelo menos, a quantidade de firewalls registrados na gerência;
- Rápida identificação e visualização gráfica dos elementos de segurança da rede;
- Interface amigável (web ou não), que permita executar as ações de configuração e monitoração dos equipamentos e políticas de segurança (tabelas, gráficos, janelas etc);
- A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC;
- Acompanhamento e implementação de usuários, grupos de usuários, definição de políticas de acesso e monitoração do acesso;
- Deve permitir diferentes perfis de gerenciamento RBAC, aplicando a segregação em diferentes perfis: read only, read write, políticas e motores de inspeções IPS;
- Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;
- Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência;
- Deve permitir auto recuperação de configurações em caso de perda de comunicação entre os Firewalls e a gerência centralizada, durante aplicação de configurações;
- Acompanhamento e implementação de operações tais como backup de configurações (regras), gerenciamento de modificações e análise de logs;
- Monitoração do firewall em tempo real, de alertas de invasões, de análise de tráfego atípico, detecção de scans, spoofing, tentativas de autenticação fracassadas ou Denial of Service (DoS), etc;
- Ações corretivas, relacionadas a eventos de emergência, tais como falhas no firewall, possíveis intrusões que comprometam a política de segurança da empresa, ou ainda uma não resposta do firewall;
- Emissão de relatórios de ataques e/ou configurações;
- O uso de criptografia entre a plataforma de gerenciamento e os firewalls, para comunicação, configuração e gerência;
- Visualização do status atual dos firewalls, tarefas pendentes e mensagens de log de forma central em tempo real, além dos relatórios gráficos dos firewalls e atividades da rede por firewall;
- A recuperação de backup num evento de falha ou erros na configuração e/ou implementação da política de segurança dos firewalls;

- Fornecimento de relatórios gráficos do firewall e atividades de rede, além de dados históricos e em tempo real, oferecendo uma visão das ocorrências na rede;
- Monitoração de processos em tempo real, ou seja, da utilização da unidade central de processamento (CPU) do firewall e/ou de processos;
- Monitoração, em tempo real, dos tráfegos detectados como: acessos web, aplicações, IPS, vírus, spyware e/ou VPN;
- As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes deverão ser visíveis na solução de gerência;
- Permitir acesso concorrente de administradores;
- Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
- Possuir interface baseada em linha de comando ou web para administração da solução de gerência;
- Bloquear alterações no mesmo item, no caso acesso simultâneo de dois ou mais administradores;
- Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários e/ou alteração de configurações;
- Gerar alertas automáticos via Email;
- Gerar alertas automáticos via SNMP;
- O gerenciamento deve possibilitar a criação e administração de políticas de NGFW e controle de aplicação;
- O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL e Filtro de DNS;
- Deve possuir a funcionalidade de workflow na criação de regras para todos os Firewalls, garantindo, o modelo de boas práticas de gestão controlada para definição de novas regras e aprovação por equipes de compliance distintas;
- Deve permitir usar palavras chaves ou cores para facilitar identificação de regras;
- Permitir localizar quais regras um objeto está sendo utilizado;
- Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;
- Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia;
- Permitir criação de regras que fiquem ativas em horário definido;
- Permitir criação de regras com data de agendamento e/ou expiração;
- Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada;

- Permitir backup das configurações e rollback de configuração para a última configuração e/ou backup salvo
- Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing)
- Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência
- Um sistema de backup/restore de todas as configurações da solução de gerência deve estar incluso e deve permitir ao administrador agendar backups
- Deve ser permitido ao administrador fazer download dos backups armazenados na ferramenta de gerenciamento
- Cada appliance de gerência deve ser hospedado em um equipamento independente, não exercendo funções de firewall;
- A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta;
- A solução deve possibilitar a distribuição e instalação remota, de novas versões de software dos appliances;
- Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS;
- Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de usuários de base externa LDAP;
- Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS;
- Deve suportar sincronização do relógio interno via protocolo NTP;
- Deve registrar login ou tentativa de login de qualquer usuário;
- Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados;
- Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade;
- Os manuais podem ser fornecidos de forma impressa ou virtual;
- O fornecimento virtual dos manuais pode ser feito através de mídia física, e-mail ou site oficial do fabricante;
- Suportar SNMP versão 2 e versão 3 ou possibilitar o gerenciamento via hypervisor nos equipamentos de gerência;
- Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como licenças, horário do sistema e firmware;
- Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

- Permitir centralização de comunicação dos Firewalls e a base de repositório de assinaturas, utilizando o gerenciador como ponto único para: distribuição de atualizações de software, assinaturas, ciclo de vida e contratos com o fabricante;
- Deve permitir especificar quais os endereços IPs têm acesso à interface de administração e gerência;
- Deve permitir ver em tempo real os logs recebidos;
- Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3, de pelo menos 3 appliances;

#### 4.1.2. SOLUÇÃO GERÊNCIA CENTRALIZADA DE FIREWALL (APPLIANCE FÍSICO)

##### 4.1.2.1. REQUISITOS GERAIS

- Para as soluções do tipo hardware, deve ser fornecida na forma de equipamento appliance próprio do fabricante da solução de FIREWALL;
- O equipamento deve ser novo, sem uso anterior e a solução ofertada (hardware e software) deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta, não sendo aceita solução em roadmap;
- A CONTRATADA deve fornecer licenças de uso dos softwares que compõem a solução proposta, em suas versões mais recentes, sem previsão de descontinuidade, na data de entrega da proposta;
- Por questões de compatibilidade e operação eficiente do sistema, o software ofertado deve ser do mesmo fabricante dos equipamentos que formam a toda solução de NEXT GENERATION FIREWALL;
- O software e hardware da Gerência, ofertada através de appliance físico, deverão ser fornecidos de forma a atender ao item 6 desse anexo em todos os seus códigos de Solução de Gerência Centralizada de Firewall – Hardware, pertinentes a este item 4.1.2, bem como em seus respectivos parâmetros de licenciamento (Número mínimo de FIREWALL a serem gerenciados);
- O software de gerência deve permitir acesso através de qualquer browser via HTTP ou HTTPS ou software exclusivo para tal, disponibilizado pelo fabricante;
- Deve fornecer, caso necessário, sistema gerenciador de banco de dados relacional para armazenar os logs de eventos gerados pelos NGFWs;
- Todos os softwares (gerenciamento, operacional e de apoio) devem ser fornecidos em mídia DVD devidamente licenciados e identificados com a chave de ativação ou de forma digital acessível através da web;

##### 4.1.2.2. ACESSÓRIOS E LITERATURAS TÉCNICAS (PARA CADA EQUIPAMENTO);

- Conjunto (kit) para montagem em rack de 19 polegadas;
- Cabos para todas as fontes de alimentação de energia elétrica, padrão ABNT 14136 (2P+T);
- Cabo console ou cabo Ethernet;

#### 4.1.3. SOLUÇÃO DE GERÊNCIA CENTRALIZADA DE FIREWALLS (APPLIANCE VIRTUAL)

##### 4.1.3.1. REQUISITOS GERAIS

- A solução de gerência centralizada poderá ser composta de um ou mais appliances virtuais que permita gerenciamento dos NGFWs e devem ser instalados em infraestrutura existente de VM (Virtual Machine) da CONTRATANTE.
- A CONTRATADA deve fornecer licenças de uso de todos os softwares que compõem a solução proposta, em suas versões mais recentes, sem previsão de descontinuidade, na data de entrega da proposta.
- O sistema de gerenciamento centralizado de NGFWs deve suportar expansão, através da contratação de licenças de software, visando atender um crescimento do parque de dispositivos gerenciados de forma a atender necessidades de expansão das atividades que envolvem um aumento de dispositivos gerenciados, de usuários autenticados, dentre outros motivos;
- Por questões de compatibilidade e operação eficiente do sistema, o software ofertado deve ser do mesmo fabricante dos equipamentos que formam a toda solução de NEXT GENERATION FIREWALL;
- O software de gerência deve ser fornecido com licença inicial para gerenciar, no mínimo, de forma a atender ao item 6.4 desse anexo, bem como em seus respectivos parâmetros de licenciamento, a quantidade mínima de NGFWs a serem gerenciados;
- O software de gerência deve permitir o crescimento modular da sua capacidade, em número de dispositivos gerenciados, através de “Licenças Adicionais”, de forma a atender a expansão prevista nos códigos de pacotes de expansão de licença expostos nos itens 6.5, 6.6 e 6.7 desse anexo;
- O software de gerência deve permitir acesso através de qualquer browser via HTTP/HTTPS ou software exclusivo para tal, disponibilizado pelo fabricante;

#### 4.1.3.2. ACESSÓRIOS E LITERATURAS TÉCNICAS (PARA CADA APPLIANCE VIRTUAL);

- Deve ser fornecido todos os softwares operacionais sejam necessários para a solução de gerência CENTRALIZADA DE NGFW para INFRA de Máquina Virtual existente;
- Deve fornecer, caso necessário, sistema gerenciador de banco de dados relacional para armazenar os logs de eventos gerados pelos NGFWs;

#### 4.1.4. PACOTES PARA EXPANSÃO DA SOLUÇÃO DE GERÊNCIA DE FIREWALLS (APPLIANCE VIRTUAL)

##### 4.1.4.1. CONDIÇÕES GERAIS

- A contratação de cada licença adicional permitirá expandir a capacidade de forma cumulativa de acordo com os pacotes de expansão definidos nos itens 6.5, 6.6 e 6.7 desse anexo, pertinentes a Solução de Gerência de Firewalls - Appliance Virtual;
- O appliance virtual ou conjunto destes a serem fornecidos para expansão, devem ser compatíveis aos equipamentos originais fornecidos que compõem a solução de gerenciamento centralizado de NGFWs;
- A CONTRATADA deve fornecer licenças de uso de todos os softwares que compõem a solução de expansão proposta, em suas versões mais recentes, sem previsão de descontinuidade, na data de entrega da proposta;

#### 4.2. GERÊNCIA DE RELATÓRIOS, LOGS E INCIDENTES

##### 4.2.1. REQUISITOS GERAIS

- 4.2.1.1. Solução externa a solução de gerência de firewalls, exclusiva para gerência e armazenamento dedicado para relatórios, logs e incidentes de eventos enviados ou coletados dos firewalls ofertados;
- 4.2.1.2. A solução deve ser do mesmo fabricante dos firewalls ofertados;
- 4.2.1.3. Deve ser compatível com todos os modelos de firewalls ofertados;
- 4.2.1.4. Interface amigável (web ou não), que permita executar monitoração dos equipamentos, eventos de segurança e eventos de rede;
- 4.2.1.5. Monitoração do firewall em tempo real, de alertas de invasões, de análise de tráfego atípico, detecção de scans, spoofing, tentativas de autenticação fracassadas ou Denial of Service (DoS), etc;
- 4.2.1.6. Ações corretivas, relacionadas a eventos de emergência, tais como falhas no firewall, possíveis intrusões que comprometam a política de segurança da empresa, ou ainda uma não resposta do firewall;
- 4.2.1.7. Emissão de relatórios de ataques e/ou configurações;
- 4.2.1.8. Visualização do status atual dos firewalls, tarefas pendentes e mensagens de log de forma central em tempo real, além dos relatórios gráficos dos firewalls e atividades da rede por firewall;
- 4.2.1.9. Fornecimento de relatórios gráficos do firewall e atividades de rede, além de dados históricos e em tempo real, oferecendo uma visão das ocorrências na rede
- 4.2.1.10. Monitoração, em tempo real, dos tráfegos detectados como: acessos web, aplicações, IPS, vírus, spyware e/ou VPN;
- 4.2.1.11. Fornecimento dos seguintes relatórios em formato HTML ou PDF: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias web mais acessadas;
- 4.2.1.12. Fornecimento dos seguintes relatórios ou dashboard com cruzamento de informações: máquinas acessadas x serviços bloqueados, usuários x URLs acessadas, usuários x categorias web bloqueadas;
- 4.2.1.13. Permitir acesso concorrente de administradores;
- 4.2.1.14. Possuir interface baseada em linha de comando ou web para administração;
- 4.2.1.15. Gerar alertas automáticos via Email;
- 4.2.1.16. Gerar alertas automáticos via SNMP;
- 4.2.1.17. Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados;
- 4.2.1.18. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade;
- 4.2.1.19. Suportar SNMP versão 2 e versão 3 ou possibilitar o gerenciamento via hypervisor nos equipamentos de gerência;
- 4.2.1.20. A solução deve possuir relatórios pré-definidos;
- 4.2.1.21. Possuir a capacidade de personalização de capas para os relatórios;
- 4.2.1.22. Permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log;
- 4.2.1.23. Possuir a capacidade de personalização de relatórios como barra, linha ou tabela;
- 4.2.1.24. Dever ser possível fazer download dos arquivos de logs recebidos;
- 4.2.1.25. Deve possuir agendamento para gerar e enviar automaticamente relatórios;

- 4.2.1.26. Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades;
- 4.2.1.27. Permitir o envio de maneira automática de relatórios por e-mail;
- 4.2.1.28. Deve permitir a escolha do e-mail a ser enviado para cada relatório escolhido;
- 4.2.1.29. Permitir programar a geração de relatórios, conforme calendário definido pelo administrador;
- 4.2.1.30. Deve ser possível definir filtros nos relatórios;
- 4.2.1.31. Deve ser capaz de definir os filtros ou layout do relatório, caso a solução suporte definir layouts deve incluir gráficos, inserir textos, imagens, alinhamento, quebras de páginas, definir fontes ou cores, entre outros;
- 4.2.1.32. Gerar alertas automáticos via E-mail, Syslog, SNMP e Webhook para plataformas de terceiros, incluindo ServiceNow, baseados em eventos como ocorrência como log, severidade de log, entre outros;
- 4.2.1.33. Deve exibir relatórios e Dashboards via interface gráfica, sem necessidade de conhecer linguagens de banco de dados customizados;
- 4.2.1.34. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 2.

#### 4.2.2. SOLUÇÃO DE GERÊNCIA DE RELATÓRIOS, LOGS E INCIDENTES (APPLIANCE FÍSICO)

##### 4.2.2.1. REQUISITOS GERAIS

- Para as soluções do tipo hardware, deve ser fornecida na forma de equipamento appliance próprio do fabricante da solução de FIREWALL;
- O equipamento deve ser novo, sem uso anterior e a solução ofertada (hardware e software) deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta, não sendo aceita solução em roadmap;
- A CONTRATADA deve fornecer licenças de uso dos softwares que compõem a solução proposta, em suas versões mais recentes, sem previsão de descontinuidade, na data de entrega da proposta;
- Por questões de compatibilidade e operação eficiente do sistema, o software ofertado deve ser do mesmo fabricante dos equipamentos que formam a toda solução de NEXT GENERATION FIREWALL;
- O software e hardware da Gerência, ofertada através de appliance físico, deverão ser fornecidos de forma a atender ao Item 6 desse anexo, em todos os seus códigos de Gerência de Relatórios, Logs e Incidentes – Hardware, pertinentes a este item 4.2.2, bem como em seus respectivos parâmetros de licenciamento (Quantidade mínima de Gigabytes de logs por dia);
- O software de gerência deve permitir acesso através de qualquer browser via HTTP ou HTTPS ou software exclusivo para tal, disponibilizado pelo fabricante;
- Deve fornecer, caso necessário, sistema gerenciador de banco de dados relacional para armazenar os logs de eventos gerados pelos NGFWs;
- Todos os softwares (gerenciamento, operacional e de apoio) devem ser fornecidos em mídia DVD devidamente licenciados e identificados com a chave de ativação ou de forma digital acessível através da web;

##### 4.2.2.2. ACESSÓRIOS E LITERATURAS TÉCNICAS (PARA CADA EQUIPAMENTO);

- Cabos para todas as fontes de alimentação de energia elétrica, padrão ABNT 14136 (2P+T);

- Cabo console ou cabo Ethernet.

#### 4.2.3. SOLUÇÃO DE GERÊNCIA DE RELATÓRIOS, LOGS E INCIDENTES (APPLIANCE VIRTUAL)

##### 4.2.3.1. REQUISITOS GERAIS

- A solução de gerência centralizada poderá ser composta de um ou mais appliances virtuais que permita a extração de relatórios e gerenciamento dos NGFWs e devem ser instalados em infraestrutura existente de VM (Virtual Machine) da CONTRATANTE;
- A CONTRATADA deve fornecer licenças de uso de todos os softwares que compõem a solução proposta, em suas versões mais recentes, sem previsão de descontinuidade, na data de entrega da proposta;
- A Solução de Gerência Relatórios, Logs e Incidentes (Appliance Virtual), deve suportar expansão, através da contratação de licenças de software, visando atender necessidades de expansão das atividades que envolvem um aumento Gigabyte de Logs diários;
- Por questões de compatibilidade e operação eficiente do sistema, o software ofertado deve ser do mesmo fabricante dos equipamentos que formam a toda solução de NEXT GENERATION FIREWALL;
- Caso o licenciamento também seja pela quantidade Gigabytes de logs diário armazenado, deverá ser fornecida licença que atenda ao estabelecido no subitem que se segue;
- O software de gerência deve ser fornecido com licença inicial para gerenciar, no mínimo, ao item 6.11 desse anexo, bem como em seus respectivos parâmetros de licenciamento e suporte mínimo;
- O software de gerência deve permitir o crescimento modular da sua capacidade, em quantidade de GB de Logs armazenados por dia, através de “Licenças Adicionais”, de forma a atender a expansão prevista nos códigos de pacotes de expansão de licença expostos nos itens 6.12, 6.13 e 6.14 desse anexo.
- O software de gerência deve permitir acesso através de qualquer browser via HTTP/HTTPS ou software exclusivo para tal, disponibilizado pelo fabricante

#### 4.2.4. PACOTES PARA EXPANSÃO DA SOLUÇÃO DE GERÊNCIA DE RELATÓRIOS, LOGS E INCIDENTES (APPLIANCE VIRTUAL)

##### 4.2.4.1. CONDIÇÕES GERAIS

- A contratação de cada licença adicional permitirá expandir a capacidade de forma cumulativa de acordo com os pacotes de expansão definidos nos itens 6.12, 6.13 e 6.14 desse anexo;
- Deverá expandir a capacidade de armazenamento de GB de Logs por dia;
- Cada licença adicional permitirá expandir a capacidade nas quantidades definidas nos item 6.12, 6.13 e 6.14 desse anexo.
- A CONTRATADA deve fornecer licenças de uso de todos os softwares que compõem a solução de expansão proposta, em suas versões mais recentes, sem previsão de descontinuidade, na data de entrega da proposta

## 5. REQUISITOS MÍNIMOS – FIREWALL

### 5.1. FIREWALL TAMANHO DATA CENTER – TIPO 1



- 5.1.1. Deve suportar, no mínimo, 120 Gbps de throughput de Firewall stateful
- 5.1.2. Deve suportar, no mínimo, 21 Gbps de throughput IPS
- 5.1.3. Deve suportar, no mínimo, 50 Gbps de throughput de VPN IPsec
- 5.1.4. Deve suportar, no mínimo, 20 Gbps de throughput de Inspeção SSL
- 5.1.5. Deve suportar, no mínimo, 25 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes e log habilitado: firewall, controle de aplicação, IPS e antimalware.
- 5.1.6. Suporte a, no mínimo, 20 milhões de conexões simultâneas
- 5.1.7. Suporte a, no mínimo, 1 milhão de novas conexões por segundo
- 5.1.8. Estar licenciado para, ou suportar sem o uso de licença, 12 mil túneis de VPN IPsec Site-to-Site simultâneos
- 5.1.9. Estar licenciado para, ou suportar sem o uso de licença, 6 mil túneis de clientes VPN IPsec simultâneos
- 5.1.10. Estar licenciado para, ou suportar sem o uso de licença, 6 mil clientes de VPN SSL simultâneos
- 5.1.11. Deverá possuir 8 (oito) interfaces RJ45 10 Gigabit Ethernet
- 5.1.12. Deverá possuir 16 (dezesesseis) interfaces SFP28 25 Gigabit Ethernet
- 5.1.13. Deverá possuir 4 (quatro) interfaces QSFP28 100 Gigabit Ethernet
- 5.1.14. Estar licenciado e ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos por equipamento. Entende-se por sistema virtual lógico a possibilidade de dividir um único equipamento físico em várias unidades virtuais, tendo um contexto para WAN e outro contexto para LAN, por exemplo.
- 5.1.15. Possuir fontes de alimentação com entrada 100-240V AC, 50-60Hz redundante Hot Swappable
- 5.1.16. Deve ser entregue suportando, e licenciado caso seja necessário, para alta disponibilidade do tipo ativo-Passivo, ativo-ativo e clustering para até quatro dispositivos idênticos (hardware e software).

## 5.2. FIREWALL TAMANHO GRANDE – TIPO 2

- 5.2.1. Deve suportar, no mínimo, 120 Gbps de throughput de Firewall stateful
- 5.2.2. Deve suportar, no mínimo, 19 Gbps de throughput IPS
- 5.2.3. Deve suportar, no mínimo, 35 Gbps de throughput de VPN IPsec
- 5.2.4. Deve suportar, no mínimo, 12 Gbps de throughput de Inspeção SSL
- 5.2.5. Deve suportar, no mínimo, 15 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes e log habilitado: firewall, controle de aplicação, IPS e antimalware.
- 5.2.6. Suporte a, no mínimo, 10 milhões de conexões simultâneas
- 5.2.7. Suporte a, no mínimo, 600 mil de novas conexões por segundo
- 5.2.8. Estar licenciado para, ou suportar sem o uso de licença, 5 mil túneis de VPN IPsec Site-to-Site simultâneos
- 5.2.9. Estar licenciado para, ou suportar sem o uso de licença, 2 mil túneis de clientes VPN IPsec simultâneos
- 5.2.10. Estar licenciado para, ou suportar sem o uso de licença, 2 mil clientes de VPN SSL simultâneos

- 5.2.11. Deverá possuir 14 (quatorze) interfaces RJ45 1 Gigabit Ethernet
- 5.2.12. Deverá possuir 10 (dez) interfaces SFP 1 Gigabit Ethernet
- 5.2.13. Deverá possuir 10 (dez) interfaces SFP+ 10 Gigabit Ethernet
- 5.2.14. Deverá possuir 4 (quatro) interfaces QSFP+ 40 Gigabit Ethernet
- 5.2.15. Estar licenciado e ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos por equipamento. Entende-se por sistema virtual lógico a possibilidade de dividir um único equipamento físico em várias unidades virtuais, tendo um contexto para WAN e outro contexto para LAN, por exemplo.
- 5.2.16. Possuir fonte de alimentação 100-240V AC, 50-60Hz redundante Hot Swappable
- 5.2.17. Deve ser entregue suportando, e licenciado caso seja necessário, para alta disponibilidade do tipo ativo-Passivo, ativo-ativo e clustering para até quatro dispositivos idênticos (hardware e software).

### 5.3. FIREWALL TAMANHO MÉDIO 1 – TIPO 3

- 5.3.1. Deve suportar, no mínimo, 40 Gbps de throughput de Firewall stateful
- 5.3.2. Deve suportar, no mínimo, 11 Gbps de throughput IPS
- 5.3.3. Deve suportar, no mínimo, 20 Gbps de throughput de VPN IPSec
- 5.3.4. Deve suportar, no mínimo, 7 Gbps de throughput de Inspeção SSL
- 5.3.5. Deve suportar, no mínimo, 9 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes e log habilitado: firewall, controle de aplicação, IPS e antimalware.
- 5.3.6. Suporte a, no mínimo, 7 milhões de conexões simultâneas
- 5.3.7. Suporte a, no mínimo, 450 mil de novas conexões por segundo
- 5.3.8. Estar licenciado para, ou suportar sem o uso de licença, 2 mil túneis de VPN IPSec Site-to-Site simultâneos
- 5.3.9. Estar licenciado para, ou suportar sem o uso de licença, 400 túneis de clientes VPN IPSec simultâneos
- 5.3.10. Estar licenciado para, ou suportar sem o uso de licença, 400 clientes de VPN SSL simultâneos
- 5.3.11. Deverá possuir 14 (quatorze) interfaces RJ45 1 Gigabit Ethernet
- 5.3.12. Deverá possuir 8 (oito) interfaces SFP 1 Gigabit Ethernet
- 5.3.13. Deverá possuir 8 (oito) interfaces SFP+ 10 Gigabit Ethernet
- 5.3.14. Estar licenciado e ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos por equipamento. Entende-se por sistema virtual lógico a possibilidade de dividir um único equipamento físico em várias unidades virtuais, tendo um contexto para WAN e outro contexto para LAN, por exemplo.
- 5.3.15. Possuir fontes de alimentação com entrada 100-240V AC, 50-60Hz redundante Hot Swappable
- 5.3.16. Deve ser entregue suportando, e licenciado caso seja necessário, para alta disponibilidade do tipo ativo-Passivo, ativo-ativo e clustering para até quatro dispositivos idênticos (hardware e software).

### 5.4. FIREWALL TAMANHO MÉDIO 2 – TIPO 4

- 5.4.1. Deve suportar, no mínimo, 10 Gbps de throughput de Firewall stateful
- 5.4.2. Deve suportar, no mínimo, 4,2 Gbps de throughput IPS

- 5.4.3. Deve suportar, no mínimo, 9 Gbps de throughput de VPN IPSec
- 5.4.4. Deve suportar, no mínimo, 3 Gbps de throughput de Inspeção SSL
- 5.4.5. Deve suportar, no mínimo, 2,8 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes e log habilitado: firewall, controle de aplicação, IPS e antimalware.
- 5.4.6. Suporte a, no mínimo, 2,5 milhões de conexões simultâneas
- 5.4.7. Suporte a, no mínimo, 220 mil de novas conexões por segundo
- 5.4.8. Estar licenciado para, ou suportar sem o uso de licença, 1 mil túneis de VPN IPSec Site-to-Site simultâneos
- 5.4.9. Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de clientes VPN IPSec simultâneos
- 5.4.10. Estar licenciado para, ou suportar sem o uso de licença, 200 clientes de VPN SSL simultâneos
- 5.4.11. Deverá possuir 12 (doze) interfaces RJ45 1 Gigabit Ethernet
- 5.4.12. Deverá possuir 8 (oito) interfaces SFP 1 Gigabit Ethernet
- 5.4.13. Deverá possuir 4 (quatro) interfaces SFP+ 10 Gigabit Ethernet
- 5.4.14. Estar licenciado e ter incluído sem custo adicional, no mínimo, 5 sistemas virtuais lógicos por equipamento. Entende-se por sistema virtual lógico a possibilidade de dividir um único equipamento físico em várias unidades virtuais, tendo um contexto para WAN e outro contexto para LAN, por exemplo.
- 5.4.15. Possuir fonte de alimentação com entrada 100-240V AC, 50-60Hz interna e redundante
- 5.4.16. Deve ser entregue suportando, e licenciado caso seja necessário, para alta disponibilidade do tipo ativo-ativo

## 5.5. FIREWALL TAMANHO PEQUENO 1 – TIPO 5

- 5.5.1. Deve suportar, no mínimo, 5 Gbps de throughput de Firewall stateful
- 5.5.2. Deve suportar, no mínimo, 1,4 Gbps de throughput IPS
- 5.5.3. Deve suportar, no mínimo, 2 Gbps de throughput de VPN IPSec
- 5.5.4. Deve suportar, no mínimo, 500 Mbps de throughput de Inspeção SSL
- 5.5.5. Deve suportar, no mínimo, 690 Mbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes e log habilitado: firewall, controle de aplicação, IPS e antimalware.
- 5.5.6. Suporte a, no mínimo, 600 mil de conexões simultâneas
- 5.5.7. Suporte a, no mínimo, 35 mil de novas conexões por segundo
- 5.5.8. Estar licenciado para, ou suportar sem o uso de licença, 150 túneis de VPN IPSec Site-to-Site simultâneos
- 5.5.9. Estar licenciado para, ou suportar sem o uso de licença, 40 túneis de clientes VPN IPSec simultâneos
- 5.5.10. Estar licenciado para, ou suportar sem o uso de licença, 40 clientes de VPN SSL simultâneos
- 5.5.11. Deverá possuir 10 (dez) interfaces RJ45 1 Gigabit Ethernet
- 5.5.12. Estar licenciado e ter incluído sem custo adicional, no mínimo, 3 sistemas virtuais lógicos por equipamento. Entende-se por sistema virtual lógico a possibilidade de dividir um único equipamento físico em várias unidades virtuais, tendo um contexto para WAN e outro contexto para LAN, por exemplo.

- 5.5.13. Possuir fonte de alimentação com entrada 100–240V AC, 50–60Hz.
- 5.5.14. Deve ser entregue suportando, e licenciado caso seja necessário, para alta disponibilidade do tipo ativo-ativo

## 5.6. FIREWALL TAMANHO PEQUENO 2 – TIPO 6

- 5.6.1. Deve suportar, no mínimo, 1,5 Gbps de throughput de Firewall stateful
- 5.6.2. Deve suportar, no mínimo, 900 Mbps de throughput IPS
- 5.6.3. Deve suportar, no mínimo, 500 Mbps de throughput de VPN IPSec
- 5.6.4. Deve suportar, no mínimo, 300 Mbps de throughput de Inspeção SSL
- 5.6.5. Deve suportar, no mínimo, 400 Mbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes e log habilitado: firewall, controle de aplicação, IPS e antimalware.
- 5.6.6. Suporte a, no mínimo, 200 mil de conexões simultâneas
- 5.6.7. Suporte a, no mínimo, 15 mil de novas conexões por segundo
- 5.6.8. Estar licenciado para, ou suportar sem o uso de licença, 100 túneis de VPN IPSec Site-to-Site simultâneos
- 5.6.9. Estar licenciado para, ou suportar sem o uso de licença, 15 túneis de clientes VPN IPSec simultâneos
- 5.6.10. Estar licenciado para, ou suportar sem o uso de licença, 15 clientes de VPN SSL simultâneos
- 5.6.11. Deverá possuir 5 interfaces RJ45 1 Gigabit Ethernet
- 5.6.12. Estar licenciado e ter incluído sem custo adicional, no mínimo, 3 sistemas virtuais lógicos por equipamento. Entende-se por sistema virtual lógico a possibilidade de dividir um único equipamento físico em várias unidades virtuais, tendo um contexto para WAN e outro contexto para LAN, por exemplo.
- 5.6.13. Possuir fonte de alimentação com entrada 100–240V AC, 50–60Hz.
- 5.6.14. Deve ser entregue suportando, e licenciado caso seja necessário, para alta disponibilidade do tipo ativo-ativo

## 6. **REQUISITOS MÍNIMOS – GERÊNCIA**

### 6.1. SOLUÇÃO DE GERÊNCIA CENTRALIZADA DE FIREWALL – HARDWARE - GCFRH1

- 6.1.1. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale
- 6.1.2. A solução deverá ser ofertada em appliance físico em hardware do mesmo fabricante das soluções de firewall
- 6.1.3. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato
- 6.1.4. Gerenciar, no mínimo, 25 unidades (NGFW ou Sistemas Virtuais) dos equipamentos da solução de NGFW de forma simultânea
- 6.1.5. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
- 6.1.6. Possuir no mínimo, 4 TB, de capacidade de storage
- 6.1.7. Deve ser suportar configuração Master/Slave de alta disponibilidade em camada 3

- 6.1.8. Deverá possuir 4 (quatro) interfaces RJ45 1 Gigabit Ethernet
- 6.1.9. Possuir fonte de alimentação com entrada 100–240V AC, 50–60Hz.

## 6.2. SOLUÇÃO DE GERÊNCIA CENTRALIZADA DE FIREWALL – HARDWARE – GCFRH2

- 6.2.1. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale
- 6.2.2. A solução deverá ser ofertada em appliance físico em hardware do mesmo fabricante das soluções de firewall
- 6.2.3. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato
- 6.2.4. Gerenciar, no mínimo, 150 unidades (NGFW ou Sistemas Virtuais) dos equipamentos da solução de NGFW de forma simultânea
- 6.2.5. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
- 6.2.6. Possuir no mínimo, 20 TB, de capacidade de storage
- 6.2.7. Deve ser suportar configuração Master/Slave de alta disponibilidade em camada 3
- 6.2.8. Deverá possuir 4 (quatro) interfaces RJ45 1 Gigabit Ethernet
- 6.2.9. Deverá possuir 2 (duas) interfaces SFP 1 Gigabit Ethernet
- 6.2.10. Possuir fonte interna 100–240V AC

## 6.3. SOLUÇÃO DE GERÊNCIA CENTRALIZADA DE FIREWALL – HARDWARE – GCFRH3

- 6.3.1. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale
- 6.3.2. A solução deverá ser ofertada em appliance físico em hardware do mesmo fabricante das soluções de firewall
- 6.3.3. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato
- 6.3.4. Gerenciar, no mínimo, 1000 unidades (NGFW ou Sistemas Virtuais) dos equipamentos da solução de NGFW de forma simultânea
- 6.3.5. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
- 6.3.6. Possuir no mínimo, 20 TB, de capacidade de storage
- 6.3.7. Deve ser suportar configuração Master/Slave de alta disponibilidade em camada 3
- 6.3.8. Deverá possuir 2 (duas) interfaces RJ45 10 Gigabit Ethernet
- 6.3.9. Deverá possuir 2 (duas) interfaces SFP+ 10 Gigabit Ethernet
- 6.3.10. Possuir fonte interna 100–240V AC redundante e hot swappable

## 6.4. SOLUÇÃO DE GERÊNCIA CENTRALIZADA DE FIREWALL - APPLIANCE VIRTUAL – GCVA

- 6.4.1. A solução deve ser baseada em appliance virtual do mesmo fabricante da solução de NGFW, e ter como objetivo gerenciar de modo centralizado todos os equipamentos a partir de uma única

console de administração;

6.4.2. Para appliance virtual, deve ser compatível com os hypervisors VMWare 6.5 e superiores, Hyper-V 2016 e superiores, e KVM.

6.4.3. Deverá estar devidamente licenciada para:

- Gerenciar, no mínimo, 10 unidades (NGFW ou Sistemas Virtuais) dos equipamentos da solução de NGFW de forma simultânea;
- Não deverá existir limite de licenciamento para o número de vCPUs no appliance virtual;
- Não deverá existir limite de licenciamento para a expansão da memória RAM no appliance virtual;

6.4.4. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.

6.4.5. Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico.

6.4.6. A solução não pode cessar, mesmo com o fim do contrato de suporte e manutenção, sendo somente a perda de suporte, atualizações e garantias suspensas

#### 6.5. EXPANSÃO GERÊNCIA CENTRALIZADA DE FIREWALL, GCVA – GCVAEXP1

6.5.1. Pacote de licenciamento para aumento da quantidade de Firewalls e Sistemas Virtuais suportados pela solução de gerência centralizada de firewall **GCVA**;

6.5.2. Deverá expandir em no mínimo 10 unidades de Firewall ou sistemas virtuais;

6.5.3. A expansão não pode cessar, mesmo com o fim do contrato de suporte e manutenção, sendo somente a perda do suporte, atualizações e garantias suspensas

#### 6.6. EXPANSÃO GERÊNCIA CENTRALIZADA DE FIREWALL, GCVA – GCVAEXP2

6.6.1. Pacote de licenciamento para aumento da quantidade de Firewalls e Sistemas Virtuais suportados pela solução de gerência centralizada de firewall **GCVA**;

6.6.2. Deverá expandir em no mínimo 50 unidades de Firewall ou sistemas virtuais;

6.6.3. A expansão não pode cessar, mesmo com o fim do contrato de suporte e manutenção, sendo somente a perda do suporte, atualizações e garantias suspensas

#### 6.7. EXPANSÃO GERÊNCIA CENTRALIZADA DE FIREWALL, GCVA – GCVAEXP3

6.7.1. Pacote de licenciamento para aumento da quantidade de Firewalls e Sistemas Virtuais suportados pela solução de gerência centralizada de firewall **GCVA**;

6.7.2. Deverá expandir em no mínimo 100 unidades de Firewall ou sistemas virtuais;

6.7.3. A expansão não pode cessar, mesmo com o fim do contrato de suporte e manutenção, sendo somente a perda do suporte, funcionalidades que necessitem de atualizações e garantias suspensas

#### 6.8. SOLUÇÃO DE GERÊNCIA DE RELATÓRIOS, LOGS E INCIDENTES- HARDWARE – GCRLIH1

- 6.8.1. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale
- 6.8.2. A solução deverá ser ofertada em appliance físico em hardware do mesmo fabricante das soluções de firewall
- 6.8.3. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato
- 6.8.4. A solução deve suportar receber, no mínimo, 25 GB de logs diários;
- 6.8.5. Possuir no mínimo, 2 TB, de capacidade de storage
- 6.8.6. Deve ser suportar configuração Master/Slave de alta disponibilidade em camada 2
- 6.8.7. Deverá possuir 2 (duas) interfaces RJ45 1 Gigabit Ethernet
- 6.8.8. Possuir fonte interna ou externa 100–240V AC

6.9. SOLUÇÃO DE GERÊNCIA DE RELATÓRIOS, LOGS E INCIDENTES- HARDWARE – GCRLIH2

- 6.9.1. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale
- 6.9.2. A solução deverá ser ofertada em appliance físico em hardware do mesmo fabricante das soluções de firewall
- 6.9.3. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato
- 6.9.4. A solução deve suportar receber, no mínimo, 100 GB de logs diários;
- 6.9.5. Possuir no mínimo, 4 TB, de capacidade de storage
- 6.9.6. Deve ser suportar configuração Master/Slave de alta disponibilidade em camada 2;
- 6.9.7. Deverá possuir 4 (quatro) interfaces Gigabit Ethernet
- 6.9.8. Possuir fonte interna 100–240V AC.

6.10. SOLUÇÃO DE GERÊNCIA DE RELATÓRIOS, LOGS E INCIDENTES- HARDWARE – GCRLIH3

- 6.10.1. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale
- 6.10.2. A solução deverá ser ofertada em appliance físico em hardware do mesmo fabricante das soluções de firewall
- 6.10.3. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato
- 6.10.4. A solução deve suportar receber, no mínimo, 600 GB de logs diários;
- 6.10.5. Possuir no mínimo, 24 TB, de capacidade de storage
- 6.10.6. Deve ser suportar configuração Master/Slave de alta disponibilidade em camada 2;
- 6.10.7. Deverá possuir 4 (quatro) interfaces 10 Gigabit Ethernet
- 6.10.8. Possuir fonte interna 100–240V AC redundante e hot swappable

6.11. SOLUÇÃO DE GERÊNCIA DE RELATÓRIOS, LOGS E INCIDENTES- APPLIANCE VIRTUAL – GCRLIVA

6.11.1. A solução deve ser baseada em appliance virtual do mesmo fabricante da solução de NGFW, e ter como objetivo gerenciar de modo centralizado todos os equipamentos a partir de uma única console de administração

6.11.2. Para appliance virtual, deve ser compatível com os hipervisores VMWare 6.5 e superiores, Hyper-V 2016 e superiores, e KVM

6.11.3. Deverá estar devidamente licenciada para:

- Suportar, no mínimo, 25 GB de logs por dia
- Não deverá existir limite de licenciamento para o número de vCPUs no appliance virtual
- Não deverá existir limite de licenciamento para a expansão da memória RAM no appliance virtual

6.11.4. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução

6.11.5. Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico

6.11.6. A solução não pode cessar, mesmo com o fim do contrato de suporte e manutenção, sendo somente a perda de suporte, funcionalidades que necessitem de atualizações e garantias suspensas

## 6.12. EXPANSÃO GERÊNCIA DE RELATÓRIOS, LOGS E INCIDENTES, GCRLIVA - GCRLIVAEXPL1

6.12.1. Pacote de licenciamento para aumento da quantidade de Firewalls e Sistemas Virtuais suportados pela solução de gerência centralizada de firewall **GCRLIVA**;

6.12.2. Deverá expandir em, no mínimo, 5 GB de logs por dia

6.12.3. A expansão não pode cessar, mesmo com o fim do contrato de suporte e manutenção, sendo somente a perda do suporte, atualizações e garantias suspensas

## 6.13. EXPANSÃO GERÊNCIA DE RELATÓRIOS, LOGS E INCIDENTES, GCRLIVA – GCRLIVAEXPL2

6.13.1. Pacote de licenciamento para aumento da quantidade de Firewalls e Sistemas Virtuais suportados pela solução de gerência centralizada de firewall **GCRLIVA**;

6.13.2. Deverá expandir em, no mínimo, 25 GB de logs por dia

6.13.3. A expansão não pode cessar, mesmo com o fim do contrato de suporte e manutenção, sendo somente a perda do suporte, atualizações e garantias suspensas

## 6.14. EXPANSÃO GERÊNCIA DE RELATÓRIOS, LOGS E INCIDENTES, GCRLIVA – GCRLIVAEXPL3

6.14.1. Pacote de licenciamento para aumento da quantidade de Firewalls e Sistemas Virtuais suportados pela solução de gerência centralizada de firewall **GCRLIVA**;

6.14.2. Deverá expandir em, no mínimo, 100 GB de logs por dia

6.14.3. A expansão não pode cessar, mesmo com o fim do contrato de suporte e manutenção, sendo somente a perda do suporte, atualizações e garantias suspensas

## 7. **TRANSCEPTORES E CABOS**

### 7.1. TRANSCEPTORES



- 7.1.1. Os transceptores ofertados e entregues, deverão ser do mesmo fabricante da solução de firewall entregue nesse edital, assim garantindo total compatibilidade e suporte;
- 7.1.2. Os transceptores devem ser novos e sem utilização anterior;
- 7.1.3. Os modelos ofertados e entregues, deverão estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta.
- 7.1.4. O Módulo Transceptor QSFP28, deve suportar conexões 100GE, suportar fibra óptica multimodo, de curto alcance, sendo completamente compatível com o firewall do Tipo 1;
- 7.1.5. O Módulo Transceptor QSFP+, deve suportar conexões de 40GE, suportar fibra óptica multimodo, de curto alcance, sendo completamente compatível com o firewall do Tipo 2;
- 7.1.6. O Módulo Transceptor SFP28, deve suportar conexões 25GE, suportar fibra óptica multimodo, de curto alcance, sendo completamente compatível com o firewall do Tipo 1;
- 7.1.7. O Módulo Transceptor SFP+, deverá suportar conexões 10GE, suportar fibra óptica multimodo, sendo completamente compatível com os firewalls dos Tipos 1, 2, 3 e 4;
- 7.1.8. O Módulo Transceptor SFP, deverá suportar conexões 1GE, fibra óptica multimodo, sendo completamente compatível com os firewalls dos Tipos 1, 2, 3 e 4;

7.2. **CORDÃO ÓPTICO MM 50/125 OM4 LC DUPLEX LSZH**

- 7.2.1. Deve ser fornecido cordão ópticos duplex, multimodo 50/125 mm, otimizada a laser OM4, novo e sem uso anterior. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta.
- 7.2.2. O cordão óptico deve ter pelo menos 3 (três) metros de comprimento.
- 7.2.3. Deve possuir revestimento externo em PVC não propagante à chama (classe de flamabilidade LSZH - Low Smoke Zero Halogen).

**8. GARANTIA E ASSISTÊNCIA TÉCNICA**

8.1. **CONDIÇÕES GERAIS**

- 8.1.1. Todos os PRODUTOS especificados neste documento deverão possuir garantia e assistência técnica pelo período de 60 meses do Fabricante, para cada tipo de Firewall, para cada tipo de Gerência de Firewall e Gerência de Relatórios, Logs e Incidentes, contado a partir do aceite da instalação deles;
- 8.1.2. A assistência técnica da garantia é de responsabilidade única e exclusiva da CONTRATADA e ocorrerá por conta da CONTRATADA, sem nenhum ônus adicional além do valor contratado, durante o período de vigência da garantia, para qualquer tipo de serviço necessário para o cumprimento do contrato;
- 8.1.3. A CONTRATANTE deve ter acesso direto ao suporte técnico 24 (vinte e quatro horas) por dia durante os 7 (sete) dias da semana, especializado do fabricante dos PRODUTOS (technical assistance center) para solução de problemas e encaminhamento de problemas ao setor competente do fabricante dos PRODUTOS;
- 8.1.4. O Fabricante deve possuir centro de atendimento técnico no Brasil;
- 8.1.5. A CONTRATADA será responsável pelo acompanhamento de chamados técnicos junto aos centros de suporte técnico do fabricante, bem como o acompanhamento da resolução desses chamados e implantação das soluções sugeridas pelo fabricante;
- 8.1.6. O serviço de assistência técnica deverá ser prestado nos respectivos locais de instalação dos PRODUTOS (on-site) caso evidenciado problema físico ou sem acesso externo ao equipamento;
- 8.1.7. O período de disponibilidade para execução, pela CONTRATADA, do serviço de assistência técnica on-site para todos os PRODUTOS é das 8h00 às 18h00, de segunda-feira a sexta-feira, exceto feriados;

8.1.8. Com o objetivo de manter os equipamentos a serem fornecidos em boas condições de funcionamento ou restabelecê-lo a tais condições, a CONTRATADA prestará serviço de assistência técnica on-site durante o período de disponibilidade, estabelecido no subitem anterior;

8.1.8.1. O prazo para a CONTRATADA iniciar o atendimento remoto, via suporte telefônico, para diagnosticar o problema é de, no máximo, 30 (trinta) minutos, contado a partir da abertura do chamado e dentro do período de disponibilidade;

8.1.8.2. O atendimento no local (on-site) deverá ser realizado no prazo máximo de 1 (um) dia útil para todos os PRODUTOS, contado a partir da abertura do chamado e dentro do período de disponibilidade;

8.1.8.3. A solução definitiva do problema deverá ocorrer no prazo máximo de 2 (dois) dias úteis, contado a partir da descoberta da causa raiz do problema;

8.1.9. A assistência técnica da garantia deverá abranger a manutenção corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive, não se restringindo a substituição de peças, partes, componentes e acessórios;

8.1.9.1. A CONTRATADA será responsável pela entrega e instalação das peças de substituição, retirada das peças com defeitos e, se necessário, deverá efetuar a reinstalação e/ou reconfiguração do sistema operacional do equipamento;

8.1.10. Todas as peças serão fornecidas à base de permuta, sendo que a reposição deverá ser feita por peças do mesmo modelo ou por modelo comprovadamente superior (neste caso, o equipamento deve ter características compatíveis), sem custos à CONTRATANTE, nos seguintes termos:

8.1.10.1. A entrega das peças ou equipamentos para reposição, deve ser efetuada em no máximo 1 dia, para a região metropolitana de São Paulo;

8.1.10.2. A entrega das peças ou equipamentos para reposição, deve ser efetuada em no máximo 2 dias, para as regiões fora da área metropolitana de São Paulo;

8.1.11. A assistência técnica on-site deverá ser executada por técnicos treinados e certificados, com qualificação técnica para diagnóstico e solução dos problemas, bem como para substituição das peças e reconfiguração dos equipamentos;

8.1.11.1. A CONTRATADA deverá possuir em seu quadro de funcionários pelo menos 2 (dois) técnicos de TI certificados pelo fabricante dos equipamentos na solução ofertada, durante toda a vigência da garantia;

8.1.12. Em caso de problemas de falhas de software (bugs), cuja solução dependa da liberação de nova versão ou patches de correção pelo fabricante, a CONTRATADA deve providenciar uma solução de contingência, no prazo máximo de 2 (dois) dias úteis contado a partir da descoberta da causa raiz;

8.1.12.1. Solução de contingência é uma solução temporária para um problema que não elimina a sua causa raiz. Esta solução restabelece a disponibilidade do ambiente, possibilitando assim a execução plena de suas funções originais, mantendo o nível de desempenho anterior ao problema;

8.1.12.2. Em caso de adoção de solução de contingência, sem prejuízo da solução definitiva cabível, a CONTRATADA deverá emitir laudos, na periodicidade exigida pela CONTRATANTE, informando sobre a evolução dos trabalhos para solucionar o problema de forma definitiva;

8.1.12.3. A solução de contingência não caracterizará a conclusão de um chamado, contudo suspenderá a contagem de tempo para a resolução de ocorrência;

8.1.12.4. A solução definitiva para problemas de falhas de software (bugs) deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias, excepcionalmente podendo ser prorrogado por iguais períodos desde que devidamente justificada por escrito pelo próprio fabricante, detalhando as ações que foram tomadas;

8.1.13. Um chamado somente será considerado concluído (solução definitiva) ou contingenciado (solução temporária) com o aceite da CONTRATANTE;

8.1.14. A CONTRATADA deverá assegurar a assistência técnica necessária à satisfatória utilização dos equipamentos, no que consiste à manutenção de hardware, instalação, reinstalação e atualização de softwares/firmwares internos dos equipamentos;

8.1.15. A CONTRATADA deverá disponibilizar, durante todo o período de vigência da garantia, acesso automático às documentações e às versões de manutenção e atualizações de softwares/firmwares dos PRODUTOS, via portal web Internet do fabricante, sob demanda, sem ônus adicional à CONTRATANTE;

8.1.16. A assistência técnica deve cobrir atendimento telefônico, sem limitação, durante a vigência da garantia;

8.1.17. Caso o equipamento, no todo ou em parte, tenha que ser retirado do local ou o tempo para reparo e solução, contado a partir do chamado, seja superior a 2 (dois) dias úteis, a CONTRATADA deverá substituir, no ato, o equipamento por outro equivalente (equipamento back-up), enquanto perdurar o conserto.

8.1.17.1. Em caso de necessidade de substituição temporária de algum equipamento, o substituto deverá ser de modelo equivalente, ser compatível e ter a mesma configuração ou superior.

8.1.17.2. Em caso de substituição permanente, o equipamento substituto deverá ter, também, a mesma capacidade e desempenho ou superior;

8.1.17.3. Em qualquer um dos casos acima, a CONTRATANTE irá emitir laudo de recepção técnica atestando ou não o cumprimento dos requisitos.

8.1.17.4. A retirada do equipamento para reparo e manutenção fora das dependências da CONTRATANTE, deverá ser comunicada pela CONTRATADA, e somente se efetivará quando do preenchimento e protocolo dos documentos específicos de retirada pelos prepostos da CONTRATADA.

8.1.17.5. Correm por conta exclusiva da CONTRATADA as responsabilidades decorrentes pela retirada e devolução do equipamento, bem como todas as despesas de transporte, frete e seguro correspondentes.

8.1.17.6. O equipamento back-up deverá ser de propriedade da CONTRATADA ou por ela locado, não cabendo à CONTRATANTE, nenhuma responsabilidade na disponibilização do mesmo.

8.1.17.7. A substituição temporária de equipamento original por equipamento back-up não caracterizará a conclusão de um chamado. Isto acontecerá quando o equipamento original retornar em perfeito estado de funcionamento à instalação de origem.

8.1.17.8. Caso o equipamento seja condenado, ele deve ser substituído por um igual ou superior, conforme o 8.1.9

8.1.18. A CONTRATADA prestará os serviços de garantia nos equipamentos, independentemente dos acessórios ou outros equipamentos que estejam, a estes, conectados.

8.1.19. A CONTRATADA providenciará, a qualquer tempo, revisões de engenharia que forem classificadas como mandatórias pelo fabricante dos equipamentos, durante a vigência da garantia.

## 8.2. COMUNICAÇÕES E REGISTROS DE OCORRÊNCIAS

8.2.1. A CONTRATADA disponibilizará para a CONTRATANTE canal de comunicação, em língua portuguesa, para registro da abertura de chamados técnicos, suporte on-line e controle de atendimento; esta Central de Atendimento deverá estar disponível das 8h00 às 18h00, de segunda-feira a sexta-feira, exceto feriados.

8.2.2. Os serviços de assistência técnica da garantia on-site serão prestados pela CONTRATADA a partir do chamado recebido através de sua Central de Atendimento.

8.2.3. A CONTRATADA ao ser acionada pela CONTRATANTE, para execução de serviços, deverá fornecer o número de registro referente ao chamado.

8.2.4. A CONTRATADA disponibilizará, no mínimo, os seguintes meios para o acionamento dos serviços de assistência técnica de garantia:

- Telefone.
- Website ou E-mail.

8.2.5. Para abertura de chamados via ligações telefônicas, estas deverão ser com tarifa gratuita e o número para contato deverá ser único para todos os equipamentos, softwares e seus componentes.

8.2.6. Qualquer mudança de endereço ou nos meios de contato, do Centro de Atendimento Técnico da CONTRATADA, deverá ser imediatamente comunicada a CONTRATANTE.

8.2.7. A CONTRATADA deverá enviar à CONTRATANTE, logo após o reparo dos equipamentos, e-mail aos cuidados dos responsáveis pelo chamado e acompanhamento técnico, informando a baixa dos chamados solucionados.

8.2.8. A CONTRATADA deverá disponibilizar o acompanhamento do estado de chamados técnicos (inclusive encerramentos), atualizados, através da Internet em interface web.

8.2.9. Após a execução de cada manutenção corretiva on-site, a CONTRATADA deverá elaborar e entregar à CONTRATANTE relatório de serviço, no qual deverão constar data e hora da chegada do técnico, descrição detalhada dos defeitos reparados, peças substituídas, anotações pertinentes ao serviço executado e assinatura do técnico que efetuou o reparo, além da assinatura e identificação dos funcionários envolvidos, da CONTRATANTE e da CONTRATADA.

8.2.10. A CONTRATADA deverá fazer constar do relatório de serviço, a relação de peças substituídas (nº de série, modelo, marca e características técnicas) ou incluídas nos equipamentos, que passaram a ser propriedade da CONTRATANTE.

8.2.11. A CONTRATADA deverá fazer constar do relatório de serviço, a designação e o número de série de quaisquer equipamentos retirados, para reparos fora do local original de instalação.

## **9. SERVIÇO DE INSTALAÇÃO**

### **9.1. CONDIÇÕES GERAIS**

9.1.1. Entende-se por instalação a montagem física dos equipamentos e acessórios fornecidos, bem como a configuração lógica de todos os equipamentos e *softwares* envolvidos, de acordo com o cenário requerido pela CONTRATANTE.

9.1.2. São de responsabilidade da CONTRATADA a instalação física, a configuração lógica e os testes de pré-operação dos PRODUTOS, conforme os requisitos e condições descritos neste documento.

9.1.3. A CONTRATANTE providenciará a infraestrutura elétrica e a infraestrutura de dados nos locais de instalação dos PRODUTOS.

9.1.4. O serviço de Instalação deverá ser executado pela CONTRATADA durante o horário comercial compreendido das 8h00 às 18h00, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes.

9.1.5. Caberá a CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes, a migração e a compatibilidade dos PRODUTOS, junto com o fabricante da solução, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos PRODUTOS.

9.1.6. Caberá a CONTRATADA, a obrigatoriedade de instalar e configurar, a critério exclusivo da CONTRATANTE, as atualizações e correções de todos os *softwares* e *firmwares* fornecidos.

9.1.7. Após a assinatura do instrumento contratual, e até a entrega dos PRODUTOS, serão realizadas reuniões preparatórias, nas dependências da CONTRATANTE, com a presença de integrantes da

equipe técnica da CONTRATADA, da qual se lavrará Ata, para permitir o acompanhamento criterioso da execução do objeto.

9.1.8. A CONTRATADA, na data da 1ª reunião de acompanhamento da execução do contrato, a ser definida pela CONTRATANTE, após a assinatura do contrato, deverá apresentar sua equipe de trabalho.

9.1.9. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação.

9.1.10. A CONTRATADA, depois de concluído o serviço de instalação dos PRODUTOS, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os PRODUTOS foram instalados de acordo com o cenário requerido pela CONTRATANTE.

9.1.11. Todos os instrumentos/equipamentos necessários para a execução do serviço e testes de aceitação do serviço serão fornecidos pela CONTRATADA.

9.1.12. A CONTRATADA deverá manter, durante a fase de implantação, a equipe técnica disponível para eventuais serviços executados fora do horário de expediente sem ônus adicional para a CONTRATANTE, quando necessário e solicitado pela equipe da CONTRATANTE, ou quando for necessário executar qualquer atividade que possa interferir no funcionamento da rede existente no local da instalação. Caso o serviço tenha que ser executado fora do horário de expediente deverá ser comunicado à CONTRATADA com antecedência mínima de 48 horas.

9.1.13. A CONTRATADA deverá elaborar e manter, no local de serviço, Relatório de Instalação (RI), em formulário timbrado próprio da CONTRATADA, com registros das ordens de serviço, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da CONTRATANTE, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE.

9.1.14. Quando aprovado o funcionamento de todos os PRODUTOS, tendo como base os itens do RI para cada PRODUTO, esses PRODUTOS deverão ser considerados instalados e aptos a serem utilizados. Isso deverá ser confirmado pelo nome, matrícula, data e assinatura do representante técnico da CONTRATANTE no RI.

9.1.15. Quando não aprovado o funcionamento de qualquer PRODUTO, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação.

9.1.16. O RI não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento dos PRODUTOS, o qual deverá ser estendido ao longo de todo o período de garantia.

9.1.17. A falta de instalação completa de um ou mais PRODUTOS constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação de PRODUTOS correspondente, enquanto perdurar a instalação incompleta.

9.1.18. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA, deve elaborar a DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO contendo todas as informações da implantação: aspectos de arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação.

9.1.19. Os serviços de instalação dos equipamentos descritos nos itens 27 ao 42, na Tabela do item 2.1. desse anexo, bem como a manutenção dos mesmos e instalação de seus respectivos softwares, poderão ser subcontratados, a critério da Contratada, sem a necessidade de autorização previa por parte da Contratante.

9.1.20. A responsabilidade pela efetiva execução dos serviços perante a Contratante será da Contratada.

9.1.21. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA.

- 9.1.22. A documentação deverá ser entregue em via impressa e em meio digital.
- 9.1.23. A documentação será validada pela equipe técnica da CONTRATANTE e do Fabricante da solução ofertada.
- 9.1.24. Toda informação manuseada durante a instalação, configuração e testes são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE.

## 9.2. LOCAL E PRAZO DE INSTALAÇÃO

9.2.1. Os PRODUTOS especificados neste anexo serão instalados no âmbito do Estado de São Paulo em duas regiões: Região Metropolitana de São Paulo e Interior de São Paulo.

9.2.1.1. A Região Metropolitana de São Paulo abrange os seguintes municípios:

Arujá	Mairiporã
Barueri	Mauá
Biritiba Mirim	Mogi das Cruzes
Caieiras	Osasco
Cajamar	Pirapora do Bom Jesus
Carapicuíba	Poá
Cotia	Ribeirão Pires
Diadema	Rio Grande da Serra
Embu	Salesópolis
Embu-Guaçu	Santa Isabel
Ferraz de Vasconcelos	Santana de Parnaíba
Francisco Morato	Santo André
Franco da Rocha	São Bernardo do Campo
Guararema	São Caetano do Sul
Guarulhos	São Lourenço da Serra
Itapecerica da Serra	São Paulo
Itapevi	Suzano
Itaquaquecetuba	Taboão da Serra
Jandira	Vargem Grande Paulista
Juquitiba	

- 9.2.1.2. A Região de Interior de São Paulo abrange os demais municípios do Estado de São Paulo.
- 9.2.2. O transporte dos PRODUTOS do almoxarifado da CONTRATANTE até o local de instalação é de responsabilidade da CONTRATANTE.
- 9.2.3. A instalação dos produtos deve ter início, no máximo, até 15 dias após a entrega dos equipamentos.
- 9.2.4. A instalação dos PRODUTOS contratados deverá ocorrer no prazo máximo de 30 (trinta) dias úteis a contar da data da solicitação pela CONTRATANTE.
- 9.2.5. A CONTRATADA deverá entregar a DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO, conforme especificado no subitem 9.1.18 deste documento, no prazo máximo de 5 (cinco) dias úteis, após a conclusão da instalação, configuração e testes de pré-operação dos PRODUTOS.
- ## 9.3. EQUIPE DE TRABALHO
- 9.3.1. A CONTRATADA deverá possuir em seu quadro de funcionários pelo menos 02 (dois) técnicos de TI certificados pelo Fabricante dos PRODUTOS na solução ofertada.
- 9.3.2. Os serviços de instalação deverão ser executados e/ou supervisionados por técnico certificado pelo Fabricante dos PRODUTOS na solução proposta.

9.3.3. A CONTRATADA deverá apresentar a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços. Para comprovar a qualificação exigida, deverão ser anexados os certificados técnicos dos referidos profissionais, emitidos pelo Fabricante dos PRODUTOS ou uma Entidade Certificadora credenciada do Fabricante.

9.3.4. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, a mesma deverá proceder a sua imediata substituição a partir da solicitação da CONTRATANTE.

## **10. SERVIÇO DE TREINAMENTO**

### **10.1. DISPOSIÇÕES PRELIMINARES**

10.1.1. O objetivo do serviço de treinamento é habilitar os participantes a configurar, operar e administrar/gerenciar os PRODUTOS especificados neste documento.

10.1.2. O treinamento deve ser por aluno e unitário, e será contratado por unidade de vagas, uma para cada aluno.

10.1.3. O treinamento deve ser presencial e ser realizado em Centro de Treinamento da CONTRATADA ou nas dependências do Fabricante.

10.1.4. A CONTRATADA deverá providenciar instalações físicas, para sala de treinamento, contemplando salas com tratamento acústico, ar-condicionado, iluminação e espaço físico adequado.

- Deve ser utilizada sala de treinamento com, no máximo, 20 pessoas por curso.
- O treinamento não necessita ser dedicado, ou seja, não é exigida a exclusividade da sala de treinamento, podendo a CONTRATADA complementar, até o número máximo, com participantes de outras empresas.

10.1.5. O treinamento deverá ser executado de 2ª a 6ª feira dentro do horário comercial, ou seja, das 8h00 às 18h00 com intervalo de, no mínimo, 1 (uma) hora para o almoço.

10.1.6. O prazo máximo para realização do treinamento especificado neste documento é de 60 (sessenta) dias a contar data da solicitação pela CONTRATANTE, podendo este prazo ser prorrogado por sucessivo períodos até o atingimento mínimo de 04 (quatro) alunos por turma. Os cursos deverão ser ministrados na língua portuguesa por instrutores de comprovada experiência técnica e didática.

10.1.7. Os instrutores deverão possuir certificação do fabricante dos PRODUTOS da solução proposta pela CONTRATADA.

10.1.8. Deverá ser fornecida, no início do treinamento, apostila de acompanhamento com todo o seu conteúdo programático, para cada participante.

10.1.9. O curso deverá ser acompanhado de exercícios práticos em sala de aula, realizados com os respectivos equipamentos e softwares a serem disponibilizados pela CONTRATADA, na proporção mínima de 01 (um) recurso para cada 02 (dois) participantes.

10.1.10. Deverá ser fornecido certificado de participação para cada participante que obtiver presença mínima de 90% (noventa por cento).

### **10.2. CAPACITAÇÃO EM SOLUÇÃO DE GERÊNCIA CENTRALIZADA DE NGFW**

10.2.1. Carga horária mínima: 40 (quarenta) horas divididas em 05 (cinco) dias úteis e consecutivos.

10.2.2. Conteúdo programático mínimo:

- Instalação e operação da plataforma de gerência.
- Descrição da plataforma de gerenciamento.
- Gerenciamento e configuração de interfaces, VLANs, WANs, Zona, DNS e proxy explícito.
- Gerenciamento de performance das interfaces.
- Controle de tráfego e QoS.
- Troubleshooting.
- Operação do utilitário de gerência.
- Configurações de alta disponibilidade, SNMP, mensagens de alerta, Configuração de traps, thresholds e alarmes de rede LAN.
- Criação de políticas de firewall, objetos, IP pool e NAT/VIP.
- Visualização de eventos.
- Administração geral, múltiplos administradores e certificados
- Gerenciamento de múltiplos firewalls (políticas, status, ocorrências, etc.) através do software de gerenciamento central
- Geração de relatórios

### 10.3. CAPACITAÇÃO EM SOLUÇÃO DE FIREWALL

#### 10.3.1. MÓDULO 1 - CAPACITAÇÃO EM SOLUÇÃO DE *FIREWALL*

10.3.1.1. Carga horária mínima: 40 (quarenta) horas divididas em 05 (cinco) dias úteis e consecutivos.

10.3.1.2. Conteúdo programático mínimo:

- Visão geral e configuração inicial.
- *Log* e alertas.
- Políticas de *firewall*.
- Conceitos de zona, objetos, *NAT* e regras do ambiente.
- Configuração de políticas e recursos de segurança.
- Roteamento.
- Conceitos de *VPN*.
- *VPN site-to-site* e *client-to-site*.
- Métodos de autenticação suportados.
- Autenticação *LDAP* e integração com o *Microsoft Active Directory*.
- Certificado Digital.



- HA - Alta Disponibilidade.
- Modo Transparente.
- NGFW – Next Generation Firewall.
- Conceitos de antivírus de gateway.
- IPS - *Intrusion Prevention System*.
- Antispyware.
- Monitoramento de redes.
- Filtragem através de segmentação física.

## 11. CONDIÇÕES DE FORNECIMENTO

### 11.1. CONDIÇÕES GERAIS

11.1.1. A CONTRATADA deverá entregar os PRODUTOS adequadamente acondicionados em suas embalagens originais, protegidos contra danos de transporte e manuseio.

11.1.2. A CONTRATADA obriga-se, sem ônus adicional à CONTRATANTE, a entregar versão mais recente dos *softwares/firmwares*, a serem fornecidos, que estejam sendo comercializados no mercado na data de assinatura do contrato de fornecimento.

11.1.3. A CONTRATA deverá fornecer, juntamente com os PRODUTOS, toda a documentação técnica original, completa e atualizada, contendo os manuais e guias de utilização, não sendo aceitas cópias de qualquer tipo.

11.1.3.1. Opcionalmente a CONTRATADA poderá disponibilizar as documentações técnicas em meio eletrônico original do fabricante.

### 11.2. LOCAL E PRAZO DE ENTREGA

11.2.1. Os PRODUTOS da presente contratação deverão ser entregues, pela CONTRATADA, na unidade administrativa/almoxarifado dos órgãos contratantes, conforme planilha no Anexo I-C - LOCAIS DE ENTREGA.

11.2.2. O prazo máximo para entrega dos PRODUTOS especificados neste documento é de 90 (noventa) dias a contar da data de assinatura da ORDEM DE FORNECIMENTO a qual será emitida pela CONTRANTE em nome da CONTRATADA.

11.2.3. A CONTRATANTE deverá ser comunicada com antecedência de 1 (um) dia, da data de realização da entrega, pela CONTRATADA.

### 11.3. RECEBIMENTO PROVISÓRIO E ACEITE DEFINITIVO

11.3.1. A CONTRATANTE realizará o recebimento provisório dos produtos, no ato da entrega, nos locais e endereços indicados e acompanhados da sua respectiva nota fiscal/fatura

11.3.2. A CONTRATANTE emitirá o termo de aceite definitivo, após a constatação de que a marca, o modelo e o part number dos PRODUTOS ofertados correspondem aos propostos no ANEXO I-A e que se encontram em perfeitas condições de funcionamento;

11.3.3. O prazo máximo para emissão do termo de aceite definitivo neste anexo é de 10 dias a contar da data de entrega destes. Caso os produtos ou serviços apresentem defeito ou não atendam às

especificações técnicas básicas requeridas, o prazo de aceite será reiniciado após a solução dos problemas detectados.

11.3.4. O prazo máximo para a CONTRATADA solucionar os problemas reportados é de 10 dias a contar do comunicado da CONTRATANTE;

11.3.5. Caso haja reincidência dos problemas reportados o aceite será novamente interrompido e a CONTRATADA será comunicada para substituir o(s) PRODUTO(S) com defeito por outro(s) novo(s), no prazo máximo de 10 (dez) dias.

#### 11.4. ACEITE DO SERVIÇO DE INSTALAÇÃO

11.4.1. A CONTRATANTE emitirá o Termo de Aceite para o serviço de instalação dos PRODUTOS, após a constatação de que o serviço executado atende às especificações técnicas deste documento.

11.4.2. O prazo máximo para emissão do Termo de Aceite do serviço de instalação é de 15 dias, a contar da data de sua conclusão e apresentação pela CONTRATADA do documento “DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO”, especificado no item 9.1.18 deste documento, que deve abordar os aspectos da arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação.

11.4.3. Caso os PRODUTOS instalados não funcionem como requerido ou o documento apresentado (DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO) esteja incompleto ou incorreto, o prazo de aceite será reiniciado após a solução dos problemas detectados.

11.4.4. O prazo máximo para a CONTRATADA solucionar os problemas reportados, é de 05 (cinco) dias a contar do comunicado da CONTRATANTE.

#### 11.4.5. TERMO DE ACEITE DO SERVIÇO DE TREINAMENTO

11.4.6. A CONTRATANTE emitirá o Termo de Aceite para o serviço de treinamento, após a constatação de que o mesmo foi executado conforme especificado neste documento.

11.4.7. O prazo máximo para emissão do Termo de Aceite do serviço de treinamento especificado neste documento é de 15 (quinze) dias a contar da data de conclusão deste. Caso o serviço de treinamento não corresponda ao que foi especificado neste documento, o prazo de aceite será reiniciado após a solução dos problemas reportados.

#### 11.5. QUALIFICAÇÃO TÉCNICA DA HABILITAÇÃO

11.5.1. A Licitante deverá apresentar atestado(s) de bom desempenho anterior em contrato(s) de mesma natureza, de complexidade tecnológica e operacional igual ou superior ao objeto desta contratação, fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, que especifique(m) em seu objeto, necessariamente o cliente, tipos de produtos fornecidos e serviços realizados, com indicações das quantidades, prazo contratual, datas de início e término e local da prestação dos serviços

11.5.2. O (s) Atestado (s) devem comprovar a experiência anterior no fornecimento de pelo menos 300 equipamentos de firewall com características semelhantes aos equipamentos objeto desse termo de referência.

11.5.3. O(s) atestado(s) deverá (ão) conter a identificação da pessoa jurídica emitente bem como o nome, o cargo do signatário e telefone para contato.

#### 11.6. DO PAGAMENTO

11.6.1. Os pagamentos de cada produto, serão efetuados pela PRODESP, a partir da emissão do Termo de Aceite, bem como o cumprimento das condições do Item 11 - CONDIÇÕES DE FORNECIMENTO

desse Termo de Referência, mediante a entrega das notas fiscais/faturas pela CONTRATADA.

11.6.1.1. As notas fiscais/faturas deverão ser emitidas após o Termo de Aceite e poderão ser emitidas discriminando, de forma separada, os itens de hardware e software, tendo em vista que a tributação entre os itens é diferente.

11.6.1.2. A emissão das notas fiscais/faturas dos itens referentes aos serviços de instalação e de treinamento deverão ser feitos de forma separada após a emissão do Termo de Aceite.

11.6.1.3. A PRODESP realizará os pagamentos nos dias 5 e 20 do mês, sendo prorrogado para o dia útil subsequente, no caso de dias não úteis.

11.6.1.4. As Notas Fiscais/Faturas entregues pela CONTRATADA entre os dias 1 e 5 do mês subsequente à prestação dos serviços serão pagas no dia 5 do mês subsequente à entrega. As Notas Fiscais/Faturas entregues após o dia 5, serão pagas no dia 20 do mês subsequente à entrega. As Notas Fiscais/Faturas entregues após o dia 21, serão pagas no dia 5 do mês subsequente, fora o mês de sua entrega.

11.6.1.5. No caso de devolução de Nota Fiscal/Fatura por qualquer motivo, a reapresentação será considerada como nova solicitação para efeito de contagem do prazo de seu pagamento.

11.6.1.6. Nos casos em que os produtos, documentos e serviços entregues não estejam em conformidade com o solicitado ou apresentem defeitos de funcionamento, ou ainda, estejam incompletos, os pagamentos serão suspensos até que os problemas sejam integralmente sanados pela CONTRATADA, conforme a criticidade do problema, caberá a PRODESP a aplicação de penalidades e sanções.

## 11.7. NÍVEIS MÍNIMOS DE SERVIÇOS (NMS)

A presente contratação possui mecanismos de monitoramento e controle de qualidade que possibilitam ao CONTRATANTE remunerar a CONTRATADA na medida do cumprimento dos Níveis Mínimos de Serviço esperados, de forma a assegurar a fiel execução do contrato.

O CONTRATANTE fará o controle qualitativo da execução contratual por meio dos Níveis Mínimos de Serviço definidos .

Ao final de cada Ordem de Fornecimento será verificado pelo fiscal do contrato o atendimento dos Níveis Mínimos de Serviço de serviço e a consequente aplicação das glosas em caso de descumprimento de algum item, garantida a ampla defesa prévia.

NÍVEIS MÍNIMOS DE SERVIÇO

Nível Mínimo de Serviço (NMS)	Incidência	Descrição do NMS	Fórmula para Determinação do Impacto por não cumprimento do NMS	Penalidade
Atraso no prazo de entrega dos equipamentos	Valor unitário do equipamento	Cumprir o prazo de entrega do equipamento	Dias úteis de atraso na entrega do equipamentos	0,2% por dia útil de atraso, limitado a 5% do valor da OS
Qualidade dos Serviços de	Valor do equipamento	Instalar os equipamentos sem erros de	Número de erros técnicos	0,1% para cada atividade não cumprida

instalação dos equipamentos		execução dos serviços		totalmente, limitado a 2% do valor da cada equipamento
Atraso na Instalação dos equipamentos	Valor do equipamento	Prazo de instalação previsto no TR	Número de dias úteis de atraso	0,2% para cada dia de atraso na instalação limitado a 5% do valor do equipamento
Tempo de início de atendimento telefônico de chamado	Valor Unitário do equipamento	Início do Atendimento em até 30 min	Percentual de Indisponibilidade	0,05% por hora de indisponibilidade, limitado a 1% do valor unitário do equipamento
Tempo de início de atendimento on-site	Valor Unitário do equipamento	Início do Atendimento previsto no TR	Números de horas de atraso para início do atendimento ao chamado	0,05% por hora de atraso, limitado a 1% do valor unitário do equipamento.

## ANEXO I-A

### DECLARAÇÃO DOS PRODUTOS A SEREM FORNECIDOS

....., ..... de ..... de 2.023

À Cia de Processamento de Dados do Estado de São Paulo – **PRODESP**

Ref.: Pregão Nº. \_\_\_\_/2023

Declaro(amos), sob as penas da lei, que, o(s) equipamento(s)/produto(s)/modelo(s) ofertado(s) a seguir, para participação nesta licitação, são novos, sem utilização anterior e atende(m) a todas e a cada uma das especificações do **ANEXO I – REL.CLAB.044/2021 v.3.1**; declaro(amos) também que estou(amos) ciente(s) e concordo(amos) que, a falta de veracidade e a inconformidade do(s) bem(ns) ora ofertado(s) neste Anexo I-A com o bem licitado, detalhadamente, especificado no Anexo I, acarretará a aplicação das penalidades cabíveis, previstas neste Edital/Contrato em especial, multa prevista e suspensão da minha empresa que ficará proibida de participar de licitações/contratações da PRODESP, pelo prazo da lei.

Para a comprovação das especificações técnicas definidas no Termo de Referência apresentamos a documentação oficial do fabricante (*Datasheet* - Descritivo com principais especificações

técnicas, *Configuration Guide* - Guia de Configuração e *Quickspecs* - Folha com resumo de especificação), bem como a tabela conforme exemplo abaixo, preenchida, especificando claramente onde encontrar:

Item 1 - Firewall TAMANHO DATACENTER – Tipo 1 - Hardware			
Item do Edital	Documento	Página	Seção

Relação dos Produtos a serem fornecidos:

12. **FIREWALL**

12.1. **FIREWALL – TIPO 1**

Quanto ao FIREWALL – TIPO 1, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

12.2. **FIREWALL – TIPO 2**

Quanto ao FIREWALL – TIPO 2, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

12.3. **FIREWALL – TIPO 3**

Quanto ao FIREWALL – TIPO 3, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

12.4. **FIREWALL – TIPO 4**

Quanto ao FIREWALL – TIPO 4, informar:

Nome do Fabricante \_\_\_\_\_  
Modelo: \_\_\_\_\_  
Nº referência (*part number*): \_\_\_\_\_  
Software/Licença/Subscrição: \_\_\_\_\_

#### 12.5. **FIREWALL – TIPO 5**

Quanto ao FIREWALL – TIPO 5, informar:

Nome do Fabricante \_\_\_\_\_  
Modelo: \_\_\_\_\_  
Nº referência (*part number*): \_\_\_\_\_  
Software/Licença/Subscrição: \_\_\_\_\_

#### 12.6. **FIREWALL – TIPO 6**

Quanto ao FIREWALL – TIPO 6, informar:

Nome do Fabricante \_\_\_\_\_  
Modelo: \_\_\_\_\_  
Nº referência (*part number*): \_\_\_\_\_  
Software/Licença/Subscrição: \_\_\_\_\_

### 13. **GERÊNCIA DE FIREWALLS**

#### 13.1. **Solução de Gerência Centralizada GCFRH1 de FIREWALL (hardware e software)**

Quanto a GERÊNCIA **GCFRH1**, informar:

Nome do Fabricante \_\_\_\_\_  
Modelo: \_\_\_\_\_  
Nº referência (*part number*): \_\_\_\_\_  
Software/Licença/Subscrição: \_\_\_\_\_

#### 13.2. **Solução de Gerência Centralizada GCFRH2 de FIREWALL (hardware e software)**

Quanto a GERÊNCIA **GCFRH2**, informar:

Nome do Fabricante \_\_\_\_\_  
Modelo: \_\_\_\_\_  
Nº referência (*part number*): \_\_\_\_\_  
Software/Licença/Subscrição: \_\_\_\_\_

#### 13.3. **Solução de Gerência Centralizada GCFRH3 de FIREWALL (hardware e software)**

Quanto a GERÊNCIA **GCFRH3**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

**13.4. Solução de Gerência Centralizada GCVA de FIREWALL (Appliance Virtual licenciado)**

Quanto a GERÊNCIA **GCVA**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

**13.5. Pacote de Expansão de Gerência Centralizada GCVAEXP1 de FIREWALL (Appliance Virtual licenciado)**

Quanto a GERÊNCIA **GCVAEXP1**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

**13.6. Pacote de Expansão de Gerência Centralizada GCVAEXP2 de FIREWALL (Appliance Virtual licenciado)**

Quanto a GERÊNCIA **GCVAEXP2**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

**13.7. Pacote de Expansão de Gerência Centralizada GCVAEXP3 de FIREWALL (Appliance Virtual licenciado)**

Quanto a GERÊNCIA **GCVAEXP3**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

**14. GERÊNCIA DE LOGS**

**14.1. Solução de Gerência Centralizada GCRLIH1 de Logs e Relatórios (hardware e software)**

Quanto a GERÊNCIA **GCRLIH1**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

**14.2. Solução de Gerência Centralizada GCRLIH2 de Logs e Relatórios (hardware e software)**

Quanto a GERÊNCXIA **GCRLIH2**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

**14.3. Solução de Gerência Centralizada GCRLIH3 de Logs e Relatórios (hardware e software)**

Quanto a GERÊNCXIA **GCRLIH3**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

**14.4. Solução de Gerência Centralizada GCRLIVA de Logs e Relatórios (Appliance Virtual licenciado)**

Quanto a GERÊNCXIA **GCRLIVA**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

**14.5. Pacote de Expansão de Gerência Centralizada GCRLIVAEXPL1 de Relatórios (Appliance Virtual licenciado)**

Quanto a GERÊNCXIA **GCRLIVAEXPL1**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

**14.6. Pacote de Expansão de Gerência Centralizada GCRLIVAEXPL2 de Relatórios (Appliance Virtual licenciado)**

Quanto a GERÊNCXIA **GCRLIVAEXPL2**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_



14.7. **Pacote de Expansão de Gerência Centralizada GCRLIVAEXPL3 de Relatórios (Appliance Virtual licenciado)**

Quanto a GERÊNCXIA **GCRLIVAEXPL3**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

15. **TRANSCEPTORES**

**Módulo transceptor QSFP28**

Quanto ao **transceptor QSFP28**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

15.1. **Módulo transceptor QSFP+**

Quanto ao **transceptor QSFP+**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

15.2. **Módulo transceptor SFP28**

Quanto ao **transceptor SFP28**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

15.3. **Módulo transceptor SFP+**

Quanto ao **transceptor SFP+**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

15.4. **Módulo transceptor SFP**

Quanto ao **transceptor SFP**, informar:

Nome do Fabricante \_\_\_\_\_

Modelo: \_\_\_\_\_

Nº referência (*part number*): \_\_\_\_\_

Software/Licença/Subscrição: \_\_\_\_\_

Obs. 1: A documentação comprobatória deve ser entregue em português ou inglês, no caso de documentação em outra língua deve ser estrangeira deve ser acompanhada de tradução, por tradutor juramentado.

Obs. 2: Não serão aceitas cartas do fabricante, como condições comprobatórias de funcionalidades, performance ou qualquer qualidade técnica aos produtos e soluções ofertadas.

Obs. 3: Caso não seja comprovada algum item das especificações técnicas previstas nesse Termo de Referência, a LICITANTE será desclassificada. Uma vez desclassificada, o pregoeiro convocará o segundo colocado na etapa de lances para apresentar a proposta e documentos e, assim, sucessivamente, até ser apresentada uma proposta que atenda integralmente a todos os requisitos do Termo de Referência.

\_\_\_\_\_  
EMPRESA LICITANTE

\_\_\_\_\_  
CNPJ/MF

\_\_\_\_\_  
NOME, CARIMBO E ASSINATURA DO REPRESENTANTE(S) LEGAL(IS)

Taboão da Serra, 20 de Outubro de 2023.

**FÁBIO MORETH MARIANO**

Gerente Executivo de Negócios, Acordos e Contratos Estratégicos



Documento assinado eletronicamente por **Fabio Moreth Mariano, Gerente Executivo**, em 20/10/2023, às 16:59, conforme horário oficial de Brasília, com fundamento no [Decreto Estadual nº 67.641, de 10 de abril de 2023](#).



A autenticidade deste documento pode ser conferida no site [https://sei.sp.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **10306910** e o código CRC **4A01AE65**.

**ANEXO II**

**Descrição dos Produtos e/ou**  
**Serviços**

## ANEXO II

### DESCRIÇÃO DOS PRODUTOS E/OU SERVIÇOS

Item do Anexo I	Descrição	Qtde	Valor Unitário R\$	Subtotal R\$
4	Firewall 12 portas 1gbps RJ45, 8 portas 1gbps SFP, 4 portas SFP+, 10 gbps throughput, 2.5M conexões simultâneas, fonte redundante, onsite, SLA 24x7	2	106.698,07	213.396,14
10	Módulo Transceptor SFP+, 10GE, para fibra óptica multimodo, sendo completamente compatível com os firewalls dos Tipos 1, 2, 3 e 4	4	475,41	1.901,64
12	"Deve ser fornecido cordão ópticos duplex, multimodo 50/125 mm OM4 LC DUPLEX LSZH"	2	491,65	983,30
33	Instalação do FIREWALL Tipo 4 - Região Metropolitana de São Paulo	2	33.603,23	67.206,46
TOTAL R\$				R\$ 283.487,54

À

CIA. DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO PRODESP

REF: PREGÃO ELETRÔNICO N° 077 / 2023 - PROCESSO N° 359.00001160/2023-10

**OBJETO:** Constituição de sistema de registro de preços para a contratação futura de solução de proteção de redes com característica de Next Generation Firewall - NGFW, em conformidade com as especificações técnicas estabelecidas no Termo de Referência Anexo I.

**DADOS DA LICITANTE**

<b>Razão Social:</b> INGRAM MICRO BRASIL LTDA	
<b>CNPJ:</b> N° 01.771.935/0010-25 <b>Inscrição Estadual:</b> 083.141.58-8 <b>Inscrição Municipal:</b> 4668735	
<b>FONE:</b> (011) 3508-2222 / 3508-1622	<b>e-mail:</b> <a href="mailto:sheila.matias@ingrammicro.com">sheila.matias@ingrammicro.com</a> <a href="mailto:francisco.zanet@ingrammicro.com">francisco.zanet@ingrammicro.com</a>
<b>Endereço:</b> Rua Porto Alegre, n° 307 – Galpão 1, Módulo 1 e 2A, setor parte A – setor área EU V, CIVIT I – cep: 29175-706 - Nova Zelândia – Serra - ES	
<b>Dados Bancários:</b> Banco do Brasil	
<b>Conta Corrente:</b> 6373-8	<b>Agência:</b> 3347-2
<b>Dados dos representantes legais para assinatura do Contrato/ARP:</b> Neiva Maria da Silva	
<b>Nacionalidade:</b> Brasileira	
<b>Qualificação:</b> Procuradora	
<b>RG:</b> RG: n° 24.476.027-5 - SSP/SP	
<b>CPF:</b> 157.847.158-36	
<b>Dados do representante legal para assinatura do Contrato/ARP:</b> Francisco Augusto Zanet	
<b>Nacionalidade:</b> Brasileira	
<b>Qualificação:</b> Procurador	
<b>RG:</b> 9.447.462-x SSP/SP	
<b>CPF:</b> 010.602.688-76	

Para o cumprimento deste Pregão, ofertamos os preços conforme demonstrado no quadro abaixo:

Item	Produto/Serviço	Descrição	Unidade Medida	Qtde.	Preço Unitário	Preço Total
1	Firewall Tipo 1 Datacenter	Firewall 2 portas SFP+, 12 portas SFP28, 4 portas QSFP28, 58gbps throughput, 20M conexões simultâneas, fonte redundante, garantia onsite, SLA 24x7	UN	85	R\$ 1.159.045,49	R\$ 98.518.866,65
2	Firewall Tipo 2- Grande	Firewall 14 portas 1gbps RJ45, 10 portas 1gbps SFP, 10 portas SFP+, 4	UN	51	R\$ 860.351,33	R\$ 43.877.917,83

**INGRAM MICRO BRASIL LTDA**

CNPJ: 01.771.935/0008-00 – Rua Porto Alegre, 307 – Galpão 1, Módulo 4, área EU V; CIVIT II – Nova Zelândia – Serra/ES

**Endereço de correspondência:** Av. Chucri Zaidan, 1240, Bloco Golden, 21º andar, Vila São Francisco, CEP 04711-130 – São Paulo– SP

Fone: (11) 3508-2222|1622|2198 – Fax: (11) 5521-0925– E-mail: [governoim@ingrammicro.com](mailto:governoim@ingrammicro.com) - [www.ingrammicro.com.br](http://www.ingrammicro.com.br)

		portas QSFP+, 120 gbps throughput, 10M conexões simultâneas, fonte redundante, onsite, SLA 24x7				
3	Firewall Tipo 3 - Médio1	Firewall 14 portas 1gbps RJ45, 8 portas 1gbps SFP, 8 portas SFP+, 40 gbps throughput, 7M conexões simultâneas, fonte redundante, onsite, SLA 24x7	UN	140	R\$ 237.129,98	R\$ 33.198.197,20
4	Firewall Tipo 4 - Médio2	Firewall 12 portas 1gbps RJ45, 8 portas 1gbps SFP, 4 portas SFP+, 10 gbps throughput, 2.5M conexões simultâneas, fonte redundante, onsite, SLA 24x7	UN	297	R\$ 106.698,07	R\$ 31.689.326,79
5	Firewall Tipo 5 - Pequeno1	Firewall com 8 portas 1gbps RJ45, 5 gbps throughput, 600 mil conexões simultâneas, onsite, SLA 24x7	UN	607	R\$ 30.051,77	R\$ 18.241.424,39
6	Firewall Tipo 6 - Pequeno2	Firewall com 5 portas 1gbps RJ45, 1,5 gbps throughput, 200 mil conexões simultâneas, onsite, SLA 24x7	UN	1879	R\$ 22.708,09	R\$ 42.668.501,11
7	Módulo transceptor QSFP28	Módulo Transceptor QSFP28, 100GE, para fibra óptica multimodo, de curto alcance, sendo completamente compatível com o firewall do Tipo 1	UN	244	R\$ 5.806,02	R\$ 1.416.668,88
8	Módulo transceptor QSFP+	Módulo Transceptor QSFP+, 40GE, para fibra óptica multimodo, de curto alcance, sendo completamente compatível com o firewall do Tipo 2	UN	203	R\$ 2.381,60	R\$ 483.464,80
9	Módulo transceptor SFP28	Módulo Transceptor SFP28, 25GE, para fibra óptica multimodo, de curto alcance, sendo completamente compatível com o firewall do Tipo 1	UN	419	R\$ 3.623,32	R\$ 1.518.171,08

**INGRAM MICRO BRASIL LTDA**

CNPJ: 01.771.935/0008-00 – Rua Porto Alegre, 307 – Galpão 1, Módulo 4, área EU V; CIVIT II – Nova Zelândia – Serra/ES  
**Endereço de correspondência:** Av. Chucuri Zaidan, 1240, Bloco Golden, 21º andar, Vila São Francisco, CEP 04711-130 – São Paulo– SP  
Fone: (11) 3508-2222|1622|2198 – Fax: (11) 5521-0925– E-mail: [governoim@ingrammicro.com](mailto:governoim@ingrammicro.com) - [www.ingrammicro.com.br](http://www.ingrammicro.com.br)

10	Módulo transceptor SFP+	Módulo Transceptor SFP+, 10GE, para fibra óptica multimodo, sendo completamente compatível com os firewalls dos Tipos 1, 2, 3 e 4	UN	1857	R\$ 475,41	R\$ 882.836,37
11	Módulo transceptor SFP	Módulo Transceptor SFP, 1GE, para fibra óptica multimodo, sendo completamente compatível com os firewalls dos Tipos 1, 2, 3 e 4	UN	2272	R\$ 291,43	R\$ 662.128,96
12	Cordão óptico MM 50/125 OM4 LCduplex LSZH	Deve ser fornecido cordão ópticos duplex, multimodo 50/125 mm OM4 LC DUPLEX LSZH	UN	1452	R\$ 491,65	R\$ 713.875,80
13	Solução de Gerência Centralizada de Firewall, Hardware	Solução de Gerência Centralizada de Firewall -GCFRH1, Hardware (servidor ou appliance físico) para gerenciar no mínimo 25 Firewalls	UN	38	R\$ 150.640,24	R\$ 5.724.329,12
14	Solução de Gerência Centralizada de Firewall, Hardware	Solução de Gerência Centralizada de Firewall -GCFRH2, Hardware (servidor ou appliance físico) para gerenciar no mínimo 150 Firewalls	UN	15	R\$ 562.963,73	R\$ 8.444.455,95
15	Solução de Gerência Centralizada de Firewall, Hardware	Solução de Gerência Centralizada de Firewall GCFRH3, Hardware (servidor ou appliance físico) para gerenciar no mínimo 1.000 Firewalls	UN	10	R\$ 944.250,21	R\$ 9.442.502,10
16	Solução de Gerência Centralizada de Firewalls, Appliance Virtual licenciado	Solução de Gerência Centralizada de Firewalls - GCVA, Appliance Virtual licenciado e com capacidade para gerenciar no mínimo 10 Firewalls, para utilização em infraestrutura de Máquina Virtual já existente	UN	41	R\$ 3.997,27	R\$ 163.888,07
17	Expansão Solução de Gerência Centralizada de	Pacote de licenças GCVAEXP1 para no mínimo 10 firewalls adicionais e todas as	UN	36	R\$ 3.997,27	R\$ 143.901,72

**INGRAM MICRO BRASIL LTDA**

CNPJ: 01.771.935/0008-00 – Rua Porto Alegre, 307 – Galpão 1, Modulo 4, área EU V; CIVIT II – Nova Zelândia – Serra/ES  
**Endereço de correspondência:** Av. Chucri Zaidan, 1240, Bloco Golden, 21º andar, Vila São Francisco, CEP 04711-130 – São Paulo– SP  
 Fone: (11) 3508-2222|1622|2198 – Fax: (11) 5521-0925– E-mail: [governoim@ingrammicro.com](mailto:governoim@ingrammicro.com) - [www.ingrammicro.com.br](http://www.ingrammicro.com.br)

	Firewalls, Appliance Virtual licenciado	demais licenças que forem necessárias, para expansão da capacidade da Gerência Centralizada de Firewall, GCVA				
18	Expansão Solução de Gerência Centralizada de Firewalls, Appliance Virtual licenciado	Pacote de licenças GCVAEXP2 para no mínimo 50 firewalls adicionais e todas as demais licenças que forem necessárias, para expansão da capacidade da Gerência Centralizada de Firewall, GCVA	UN	10	R\$ 19.986,36	R\$ 199.863,60
19	Expansão Solução de Gerência Centralizada de Firewalls, Appliance Virtual licenciado	Pacote de licenças GCVAEXP3 para no mínimo 100 firewalls adicionais e todas as demais licenças que forem necessárias para expansão da capacidade da Gerência Centralizada de Firewall, GCFRVA	UN	23	R\$ 210.226,77	R\$ 4.835.215,71
20	Solução de Gerência Centralizada de Logs e Relatórios, Hardware	Solução de Gerência de Relatórios, Logs e Incidentes GCRLIH1, Hardware (servidor ou appliance físico) para gerenciar no mínimo 25GB Logs por dia	UN	42	R\$ 52.416,99	R\$ 2.201.513,58
21	Solução de Gerência Centralizada de Logs e Relatórios, Hardware	Solução de Gerência de Relatórios, Logs e Incidentes GCRLIH2, Hardware (servidor ou appliance físico) para gerenciar no mínimo 100GB Logs por dia	UN	23	R\$ 113.647,74	R\$ 2.613.898,02
22	Solução de Gerência Centralizada de Logs e Relatórios, Hardware	Solução de Gerência de Relatórios, Logs e Incidentes GCRLIH3, Hardware (servidor ou appliance físico) para gerenciar no mínimo 600GB Logs por dia	UN	22	R\$ 378.797,79	R\$ 8.333.551,38
23	Solução de Gerência Centralizada de Logs e Relatórios,	Solução de Gerência de Relatórios, Logs e Incidentes GCRLIVA - Appliance Virtual licenciado e com	UN	30	R\$ 69.818,21	R\$ 2.094.546,30

**INGRAM MICRO BRASIL LTDA**

CNPJ: 01.771.935/0008-00 – Rua Porto Alegre, 307 – Galpão 1, Módulo 4, área EU V; CIVIT II – Nova Zelândia – Serra/ES  
**Endereço de correspondência:** Av. Chucuri Zaidan, 1240, Bloco Golden, 21º andar, Vila São Francisco, CEP 04711-130 – São Paulo– SP  
 Fone: (11) 3508-2222|1622|2198 – Fax: (11) 5521-0925– E-mail: [governoim@ingrammicro.com](mailto:governoim@ingrammicro.com) - [www.ingrammicro.com.br](http://www.ingrammicro.com.br)



	Appliance Virtual licenciado	capacidade para gerenciar no mínimo 25 GB Logs por dia				
24	Expansão Solução de Gerência Centralizada de Logs e Relatórios, Appliance Virtual licenciado	Pacote de licenças GCRLIVAEXPL1 de expansão (licenças) para GCRLIVA de 5 GB de logs por dia	UN	13	R\$ 11.895,01	R\$ 154.635,13
25	Expansão Solução de Gerência Centralizada de Logs e Relatórios, Appliance Virtual licenciado	Pacote de licenças GCRLIVAEXPL2 de expansão (licenças) para GCRLIVA de 25 GB de logs por dia	UN	44	R\$ 42.956,83	R\$ 1.890.100,52
26	Expansão Solução de Gerência Centralizada de Logs e Relatórios, Appliance Virtual licenciado	Pacote de licenças GCRLIVAEXPL3 de expansão(licenças) para GCRLIVA de 100 GB de logs por dia	UN	12	R\$ 115.648,59	R\$ 1.387.783,08
27	Instalação Firewall - Tipo 1	Instalação do FIREWALL Tipo 1 - Região Metropolitana de São Paulo	UN	64	R\$ 71.742,42	R\$ 4.591.514,88
28	Instalação Firewall - Tipo 1	Instalação do FIREWALL Tipo 1 – Interior de São Paulo	UN	6	R\$ 73.232,61	R\$ 439.395,66
29	Instalação Firewall - Tipo 2	Instalação do FIREWALL Tipo 2 – Região Metropolitana de São Paulo	UN	34	R\$ 67.453,17	R\$ 2.293.407,78
30	Instalação Firewall - Tipo 2	Instalação do FIREWALL Tipo 2 – Interior de São Paulo	UN	13	R\$ 69.102,47	R\$ 898.332,11
31	Instalação Firewall - Tipo 3	Instalação do FIREWALL Tipo 3 -Região Metropolitana de São Paulo	UN	96	R\$ 36.747,79	R\$ 3.527.787,84
32	Instalação Firewall - Tipo 3	Instalação do FIREWALL Tipo 3 - Interior de São Paulo	UN	35	R\$ 37.679,04	R\$ 1.318.766,40
33	Instalação Firewall - Tipo 4	Instalação do FIREWALL Tipo 4 -Região	UN	109	R\$ 33.603,23	R\$ 3.662.752,07

**INGRAM MICRO BRASIL LTDA**

CNPJ: 01.771.935/0008-00 – Rua Porto Alegre, 307 – Galpão 1, Modulo 4, área EU V; CIVIT II – Nova Zelândia – Serra/ES  
**Endereço de correspondência:** Av. Chucuri Zaidan, 1240, Bloco Golden, 21º andar, Vila São Francisco, CEP 04711-130 – São Paulo– SP  
 Fone: (11) 3508-2222|1622|2198 – Fax: (11) 5521-0925– E-mail: [governoim@ingrammicro.com](mailto:governoim@ingrammicro.com) - [www.ingrammicro.com.br](http://www.ingrammicro.com.br)

		Metropolitana de São Paulo				
34	Instalação Firewall - Tipo 4	Instalação do FIREWALL Tipo 4 -Interior de São Paulo	UN	112	R\$ 34.227,25	R\$ 3.833.452,00
35	Instalação Firewall - Tipo 5	Instalação do FIREWALL Tipo 5 -Região Metropolitana de São Paulo	UN	235	R\$ 22.919,00	R\$ 5.385.965,00
36	Instalação Firewall - Tipo 5	Instalação do FIREWALL Tipo 5 -Interior de São Paulo	UN	360	R\$ 23.934,88	R\$ 8.616.556,80
37	Instalação Firewall - Tipo 6	Instalação do FIREWALL Tipo 6 -Região Metropolitana de São Paulo	UN	308	R\$ 20.337,37	R\$ 6.263.909,96
38	Instalação Firewall - Tipo 6	Instalação do FIREWALL Tipo 6 -Interior de São Paulo	UN	1529	R\$ 21.559,60	R\$ 32.964.628,40
39	Instalação Gerência Centralizada de Firewalls	Instalação da Gerência Centralizada de FIREWALL - Região Metropolitana de São Paulo	UN	50	R\$ 25.471,85	R\$ 1.273.592,50
40	Instalação Gerência Centralizada de Firewalls	Instalação da Gerência Centralizada de FIREWALL - Interior de São Paulo	UN	9	R\$ 28.970,14	R\$ 260.731,26
41	Instalação Gerência Centralizada de Logs e Relatórios	Instalação da Gerência Centralizada de Logs e Relatórios - Região Metropolitana de São Paulo	UN	56	R\$ 21.675,65	R\$ 1.213.836,40
42	Instalação Gerência Centralizada de Logs e Relatórios	Instalação da Gerência Centralizada de Logs e Relatórios - Região Interior de São Paulo	UN	12	R\$ 32.180,18	R\$ 386.162,16
43	Treinamento Firewall	Treinamento da Solução de FIREWALL	UN	185	R\$ 11.883,50	R\$ 2.198.447,50
44	Treinamento Gerência Firewall	Treinamento da Solução de Gerência Centralizada para FIREWALL	UN	185	R\$ 11.184,47	R\$ 2.069.126,95
<b>PREÇO GLOBAL:</b>						<b>R\$ 402.699.929,81</b>

**INGRAM MICRO BRASIL LTDA**

CNPJ: 01.771.935/0008-00 – Rua Porto Alegre, 307 – Galpão 1, Módulo 4, área EU V; CIVIT II – Nova Zelândia – Serra/ES  
**Endereço de correspondência:** Av. Chucri Zaidan, 1240, Bloco Golden, 21º andar, Vila São Francisco, CEP 04711-130 – São Paulo– SP  
 Fone: (11) 3508-2222|1622|2198 – Fax: (11) 5521-0925– E-mail: [governoim@ingrammicro.com](mailto:governoim@ingrammicro.com) - [www.ingrammicro.com.br](http://www.ingrammicro.com.br)

## **CONDIÇÕES GERAIS**

**Validade de proposta:** 60 (sessenta) dias, a partir da data de sua apresentação.

Declaremos que no valor total proposto estão englobados todos os custos e despesas previstos nesta licitação, tais como: custos diretos e indiretos, tributos, encargos sociais, trabalhistas e previdenciários, seguros, taxas, lucro, uniformes, alimentação, transporte, plano de assistência médico-hospitalar e odontológica e outros necessários ao cumprimento integral do objeto.

Serra, 28 de novembro de 2023.

NEIVA MARIA DA  
SILVA:15784715836

Assinado de forma digital por NEIVA  
MARIA DA SILVA:15784715836  
Dados: 2023.11.28 14:33:26 -03'00'

---

**INGRAM MICRO BRASIL LTDA**

Neiva Maria da Silva

Procuradora

RG: nº 24.476.027-5 / SSP/SP

CPF/MF: 157.847.158-36

FRANCISCO  
AUGUSTO  
ZANET:01060268876

Assinado de forma digital  
por FRANCISCO AUGUSTO  
ZANET:01060268876  
Dados: 2023.11.28 14:28:21  
-03'00'

---

**INGRAM MICRO BRASIL LTDA**

Francisco Augusto Zanet

Procurador

RG: nº 9.447.462 – SSP/SP

CPF/MF: 010.602.688-76

---

**INGRAM MICRO BRASIL LTDA**

CNPJ: 01.771.935/0008-00 – Rua Porto Alegre, 307 – Galpão 1, Modulo 4, área EU V; CIVIT II – Nova Zelândia – Serra/ES

**Endereço de correspondência:** Av. Chucri Zaidan, 1240, Bloco Golden, 21º andar, Vila São Francisco, CEP 04711-130 – São Paulo– SP

Fone: (11) 3508-2222|1622|2198 – Fax: (11) 5521-0925– E-mail: [governoim@ingrammicro.com](mailto:governoim@ingrammicro.com) - [www.ingrammicro.com.br](http://www.ingrammicro.com.br)

## **ANEXO III**

### **Termo de Ciência e de Notificação**

## **ANEXO IV**

### **Termo de Encerramento e Outras Avenças – Modelo**

## ANEXO IV - MODELO

### TERMO DE ENCERRAMENTO E OUTRAS AVENÇAS DO CONTRATO DE AQUISIÇÃO .....FIRMADO ENTRE A COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO – PRODESP E.....

Pelo presente termo, de um lado, a **COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP**, com sede no município de Taboão da Serra - estado de São Paulo, na Rua Agueda Gonçalves, nº 240, inscrita no CNPJ/MF nº 62.577.929/0001-35, doravante designada simplesmente **PRODESP** e, de outro lado, a empresa \_\_\_\_\_, inscrita no CNPJ/MF sob nº \_\_\_\_\_, com sede \_\_\_\_\_, doravante designada simplesmente **CONTRATADA**, representadas neste ato por seus representantes legais ao final designados e assinados, resolvem encerrar o contrato de....., mediante a seguinte cláusula e condições:

#### I – ENCERRAMENTO E OUTRAS AVENÇAS

- 1.1. As partes, de comum acordo, consideram concluído o objeto do contrato PRO.MINUTA em .... de ..... de 2....., permanecendo em plena vigência todas as obrigações eventualmente remanescentes.
- 1.2. Em decorrência do encerramento do contrato mencionado no item 1.1., as partes dão-se plena, rasa, mútua, recíproca, irrestrita, irrevogável e irretratável quitação dos serviços e valores referentes ao objeto do contrato PRO.MINUTA, para nada mais reclamar a qualquer título.

E, por estarem assim justas e contratadas, as Partes e testemunhas assinam o presente termo.

Taboão da Serra, a data de assinatura deste instrumento corresponde a data da última assinatura digital do(s) representante(s) legal(is).

### COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO – PRODESP

Nome:  
CPF:

#### CONTRATADA:

Nome:  
CPF:

#### TESTEMUNHAS:

#### PELA PRODESP

Nome:  
CPF

#### PELA CONTRATADA

Nome:  
CPF

---

**ANEXO III****CONTRATO Nº RP00124-02****TERMO DE CIÊNCIA E DE NOTIFICAÇÃO**

**CONTRATANTE:** COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM

**CONTRATADA:** INGRAM MICRO BRASIL LTDA

**CONTRATO Nº:** RP00124-02

**OBJETO:** AQUISIÇÃO DE SOLUÇÃO DE PROTEÇÃO DE REDES NGFW – NEXT GENERATION FIREWALL

**ADVOGADO(S) Nº OAB/E-MAIL:** CAIO AUGUSTO DE MORAES FORJAZ / OAB Nº 182.311 / e-mail: caio.forjaz@cptm.sp.gov.br e RAFAEL TONIATO MANGERONA / OAB Nº 213.777 / e-mail: rafael.mangerona@cptm.sp.gov.br.

Pelo presente TERMO, nós, abaixo identificados:

**1. Estamos CIENTES de que:**

- a) o ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;
- b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;
- c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;
- d) as informações pessoais dos responsáveis pela contratante e interessados estão cadastradas no módulo eletrônico do “Cadastro Corporativo TCESP – CadTCESP”, nos termos previstos no Artigo 2º das Instruções nº01/2020, conforme “Declaração(ões) de Atualização Cadastral” anexa (s);
- e) é de exclusiva responsabilidade do contratado manter seus dados sempre atualizados.

**2. Damo-nos por NOTIFICADOS para:**

- a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;
- b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

**AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:**

Nome: MICHAEL SOTELO CERQUEIRA

Cargo: Diretor Presidente

CPF: 284.295.458-08

**RESPONSÁVEIS PELA HOMOLOGAÇÃO DO CERTAME OU RATIFICAÇÃO DA DISPENSA/INEXIGIBILIDADE DE LICITAÇÃO:**

Nome: NE

Cargo: NE

CPF: NE


**RESPONSÁVEIS QUE ASSINARAM O AJUSTE:**

**Pelo contratante:**

Nome: ANA CAROLINE DE FARIA EDUARDO BORGES

Cargo: Diretora Administrativa e Financeira

CPF: 003.938.371-73

Documento assinado digitalmente  
 ANA CAROLINE DE FARIA EDUARDO BORGES  
Data: 27/12/2024 17:50:13-0300  
Verifique em <https://validar.iti.gov.br>

Nome: MICHAEL SOTELO CERQUEIRA

Cargo: Diretor Presidente


CPF: 284.295.458-08

Documento assinado digitalmente  
 MICHAEL SOTELO CERQUEIRA  
Data: 07/01/2025 19:26:48-0300  
Verifique em <https://validar.iti.gov.br>

Nome: JOSÉ LUIZ BARCI NEVES

Cargo: Gerente de Tecnologia da Informação

CPF: 853.555.507-20

Documento assinado digitalmente  
 JOSE LUIZ BARCI NEVES  
Data: 27/12/2024 17:16:40-0300  
Verifique em <https://validar.iti.gov.br>

**Pela contratada:**

Nome: NEIVA MARIA DA SILVA

Cargo: Procuradora

CPF: 157.847.158-36

NEIVA MARIA DA  
SILVA:157847158  
36  
Assinado de forma digital por  
NEIVA MARIA DA  
SILVA:15784715836  
Dados: 2024.12.27 16:37:42  
-03'00'

Nome: FRANCISCO AUGUSTO ZANET

Cargo: Procurador

CPF: 010.602.688-76

FRANCISCO  
AUGUSTO  
ZANET:01060268876  
Assinado de forma digital por  
FRANCISCO AUGUSTO  
ZANET:01060268876  
Dados: 2024.12.27 16:55:06  
-03'00'


**RESPONSÁVEL POR AÇÕES DE COORDENAÇÃO, ACOMPANHAMENTO, MONITORAMENTO, AVALIAÇÃO E FISCALIZAÇÃO:**

**Gestor do contrato:**

Nome: LEONARDO MARQUES LOPES

Cargo: Chefe do Departamento de Operação de TI

CPF: 377.303.338-99


Documento assinado digitalmente  
 LEONARDO MARQUES LOPES  
Data: 30/12/2024 09:21:56-0300  
Verifique em <https://validar.iti.gov.br>

**ORDENADOR DE DESPESAS DA CONTRATANTE:**

Nome: MICHAEL SOTELO CERQUEIRA

Cargo: Diretor Presidente

CPF: 284.295.458-08

Documento assinado digitalmente  
 MICHAEL SOTELO CERQUEIRA  
Data: 07/01/2025 19:25:20-0300  
Verifique em <https://validar.iti.gov.br>