Belo Horizonte, 11 de julho de 2024.

Aos Srs. Licitantes!

REF: PREGÃO ELETRÔNICO Nº 010/2024 (315855) – Contratação de empresa especializada para fornecimento de software, hardware, serviço de instalação, migração, configuração e otimização para solução de firewall, modelo SonicWall Gen 7 NSa 2700, com alta disponibilidade (HA – High Availability), contendo Advanced Protection Security Suite, pelo período de 36 (trinta e seis) meses, incluindo o suporte técnico do fabricante por igual período, para atender as necessidades do Sescoop / MG.

A Comissão Permanente de Licitação do Sescoop / MG, no uso de suas atribuições, acusa o recebimento de questionamentos encaminhados por empresa interessada no certame, os quais vem transcrever, esclarecer e retificar, conforme abaixo:

Questionamento 01: Referente ao início da disputa. Consta - O limite máximo para acolhimento das Propostas : 15/07/2024 até às 10hs e a Data e hora da Disputa: 15/04/2024 às 9:30 hs. Pergunta: Qual o horário do início da disputa? 9:30 ou 10Hs?

Resposta 01: Conforme previsto no edital, as propostas serão acolhidas no Portal de Compras Públicas, **até às 10h00 do dia 15/07/2024**, com a sessão pública se iniciando às 10h30 do mesmo dia. Prints abaixo:

SESCOOP / MG

EDITAL DO PREGÃO ELETRÔNICO Nº 010/2024 (315855)	
Data de divulgação: 02/07/2024, mediante inserção do edital no sítio eletrônico institucional, no endereço https://sistemaocemg.coop.br/editais/.	**Abertura**: às 10h30 em 15/07/2024 no sítio: www.portaldecompraspublicas.com.br.

- Início do Acolhimento de Propostas: **03/07/2024 às 10h00**
- Limite para Acolhimento das Propostas: **15/07/2024 até às 10h00**
- Data e hora da disputa: **15/07/2024 às 10h30**

Questionamento 02: No que tange à composição de valores, informamos que o item 3 Software Adavanced Protection Security Suite já inclui o item 4 que é a garantia de 3 anos. De posse das informações, questionamos o formato de oferecimento dos itens. Pergunta: Podemos inserir o valor zerado para o item 4, uma vez que o valor já esta inserido no item 3?

ITEM	QTDE.	DESCRIÇÃO. (A LICITANTE DEVERÁ DESCREVER, DETALHADAMENTE, OS EQUIPAMENTOS E SERVIÇOS QUE ESTÃO SENDO OFERTADOS, OBSERVANDO AS ESPECIFICAÇÕES DEFINIDAS NO ANEXO I).	VALOR UNITÁRIO	VALOR TOTAL
1	1	SonicWall Gen 7 NSa 2700 appliances 01 (ou superior do mesmo fabricante).	-	R$ ( )
2	1	SonicWall Gen 7 NSa 2700 appliances 02 (HA – High Availability).	-	R$ ( )
3	1	Software Advanced Protection Security Suite.	-	R$ ( )
4	1	Garantia do fornecedor (3 anos).	-	R$ ( )
5	1	Suporte técnico do fornecedor (3 anos).	-	R$ ( )
6	1	Serviço de instalação/migração, configuração e otimização.	-	R$ ( )
7	4	Fornecimento de 04 Cabos de Conexão Direta DAC SFP 10G 1,0 Metro.	R$ ( )	R$ ( )
VALOR GLOBAL DA PROPOSTA				R$ ( )

1) Declaramos, sob as penalidades da Lei, para fins de participação na licitação em referência, que a

Resposta 02: Considerando manifestação da Gerência de Tecnologia da Informação (GETIN), no sentido de que procede o questionamento da empresa interessada, a Comissão Permanente de Licitação resolve promover a **retificação parcial das tabelas** contendo o detalhamento dos itens a serem precificados. É importante destacar que não foram alteradas as exigências do edital, mas apenas revisada a maneira de se precificar. Assim, ficam **RETIFICADOS** os pontos do edital que tratam do tema, conforme abaixo:

RETIFICAÇÃO DO ITEM 4 DO ANEXO I (TERMO DE REFERÊNCIA):

4. ESPECIFICAÇÃO TÉCNICA DA FERRAMENTA FIREWALL:

PRODUTO SOLUÇÃO DE FIREWALL	LOTE ÚNICO / QUANTIDADE
SonicWall Gen 7 NSa 2700 appliances 01 (ou superior do mesmo fabricante) com garantia de 3 anos do fabricante.	**01**
SonicWall Gen 7 NSa 2700 appliances 02 (HA – High Availability) com garantia de 3 anos do fabricante.	
Software Advanced Protection Security Suite com suporte técnico de 3 anos do fabricante.	
~~**Garantia do fornecedor (3 anos).**~~	
~~**Suporte técnico do fornecedor (3 anos).**~~	
Serviço de instalação/migração, configuração e otimização.	
Fornecimento de 04 Cabos de Conexão Direta DAC SFP 10G 1,0 Metro.	**04**

RETIFICAÇÃO DA TABELA PARA PRECIFICAÇÃO CONSTANTE DO ANEXO II (MODELO DE CARTA PROPOSTA):

ITEM	QTDE.	DESCRIÇÃO. (A LICITANTE DEVERÁ DESCREVER, DETALHADAMENTE, OS EQUIPAMENTOS E SERVIÇOS QUE ESTÃO SENDO OFERTADOS, OBSERVANDO AS ESPECIFICAÇÕES DEFINIDAS NO ANEXO I).	VALOR UNITÁRIO	VALOR TOTAL
1	1	SonicWall Gen 7 NSa 2700 appliances 01 (ou superior do mesmo fabricante) **com garantia de 3 anos do fabricante.**	-	R$ ( )
2	1	SonicWall Gen 7 NSa 2700 appliances 02 (HA – High Availability) **com garantia de 3 anos do fabricante.**	-	R$ ( )
3	1	Software Advanced Protection Security Suite **com suporte técnico de 3 anos do fabricante**.	-	R$ ( )
~~4~~	~~1~~	~~Garantia do fornecedor (3 anos).~~	~~-~~	~~R$ ( )~~
~~5~~	~~1~~	~~Suporte técnico do fornecedor (3 anos).~~	~~-~~	~~R$ ( )~~
4	1	Serviço de instalação/migração, configuração e otimização.	-	R$ ( )
5	4	Fornecimento de 04 Cabos de Conexão Direta DAC SFP 10G 1,0 Metro.	R$ ( )	R$ ( )
VALOR GLOBAL DA PROPOSTA				**R$ ( )**

RETIFICAÇÃO DO ITEM 10.1 DO ANEXO VII (MINUTA DE CONTRATO):

10.1. Compete a CONTRATADA fornecer os seguintes itens para execução do objeto:

PRODUTO SOLUÇÃO DE FIREWALL	QUANTIDADE
SonicWall Gen 7 NSa 2700 appliances 01 (ou superior do mesmo fabricante) **com garantia de 3 anos do fabricante.**	01
SonicWall Gen 7 NSa 2700 appliances 02 (HA – High Availability) **com garantia de 3 anos do fabricante.**	
Software Advanced Protection Security Suite **com suporte técnico de 3 anos do fabricante.**	
~~Garantia do fornecedor (3 anos).~~	
~~Suporte técnico do fornecedor (3 anos).~~	
Serviço de instalação/migração, configuração e otimização.	
Fornecimento de 04 Cabos de Conexão Direta DAC SFP 10G 1,0 Metro.	04

OBSERVAÇÃO: permanecem inalteradas as demais exigências do edital.

Atenciosamente,

Misael Gomes da Silva
Pregoeiro

Robert Martins Santos
Presidente da Comissão Permanente de Licitação
Autoridade Competente

SERVIÇO NACIONAL DE APRENDIZAGEM DO COOPERATIVISMO DE MINAS GERAIS
SESCOOP / MG

EDITAL DO PREGÃO ELETRÔNICO Nº 010/2024 (315855)	
Data de divulgação: 02/07/2024, mediante inserção do edital no sítio eletrônico institucional, no endereço https://sistemaocemg.coop.br/editais/.	**Abertura**: às 10h30 em **15/07/2024** no sítio: www.portaldecompraspublicas.com.br.
OBJETO	
Contratação de empresa especializada para fornecimento de software, hardware, serviço de instalação, migração, configuração e otimização para solução de firewall, modelo SonicWall Gen 7 NSa 2700, com alta disponibilidade (HA – High Availability), contendo Advanced Protection Security Suite, pelo período de 36 (trinta e seis) meses, incluindo o suporte técnico do fabricante por igual período, para atender as necessidades do Sescoop / MG.	
ORIENTAÇÕES IMPORTANTES:	
1. O Serviço Nacional de Aprendizagem do Cooperativismo – SESCOOP – é uma instituição integrante do **Sistema S**, sendo esta Licitação regida pelo Regulamento de Licitações e Contratos do SESCOOP, aprovado pela Resolução nº 2056/2023 do Conselho Nacional do SESCOOP, datada de 25 de setembro de 2023. **O SESCOOP / MG tem natureza privada e não integra a administração pública direta ou indireta, sem se submeter à Lei 14.133/2021.** 2. Este Pregão será conduzido no modo de disputa **ABERTO E FECHADO**, ou seja, hipótese em que as licitantes deverão apresentar lances públicos e sucessivos, com lance final e fechado. Portanto, alertamos às licitantes interessadas em participar deste Pregão Eletrônico que **é necessário anexar previamente a proposta e os documentos de habilitação**, exclusivamente por meio de campo próprio do sistema, após o registro de sua proposta no Sistema do Portal de Compras Públicas, disponível em www.portaldecompraspublicas.com.br. 3. Informamos ainda que o Pregão Eletrônico nº 010/2024 (**315855**) possui critério de julgamento MENOR PREÇO GLOBAL. 4. Dessa forma, os licitantes interessados deverão se atentar para cadastrarem o valor da proposta inicial e enviarem os lances **CONSIDERANDO O VALOR GLOBAL.** 5. A proposta inicial poderá ser apresentada exclusivamente no sistema e a proposta final ajustada ao lance vencedor deverá ser encaminhada após solicitação do Pregoeiro.	
A leitura destas orientações não dispensa, em hipótese alguma, a análise e compreensão na íntegra do Edital do Pregão Eletrônico nº 010/2024 (315855) e seus anexos.	
Registro de Preços	**Vistoria**
NÃO	NÃO
Instrumento Contratual	**Forma de Adjudicação**
Contrato de Fornecimento	Menor preço global
Exigência de Amostra	**Modo de Disputa**
NÃO	Aberto e Fechado

EDITAL DO PREGÃO ELETRÔNICO Nº 010/2024 (315855)

O **SERVIÇO NACIONAL DE APRENDIZAGEM DO COOPERATIVISMO DE MINAS GERAIS – SESCOOP / MG**, sediado na Rua Ceará, nº 771, bairro Santa Efigênia, CEP 30.150-312, em Belo Horizonte – MG., inscrito no CNPJ sob o nº 07.064.534/0001-20, por intermédio de seu Pregoeiro e membros da equipe de apoio, torna público para conhecimento dos interessados, que irá realizar Licitação na modalidade de PREGÃO ELETRÔNICO, cujo objeto é a **Contratação de empresa especializada para fornecimento de software, hardware, serviço de instalação, migração, configuração e otimização para solução de firewall, modelo SonicWall Gen 7 NSa 2700, com alta disponibilidade (HA – High Availability), contendo Advanced Protection Security Suite, pelo período de 36 (trinta e seis) meses, incluindo o suporte técnico do fabricante por igual período, para atender as necessidades do Sescoop / MG.**, conforme termos e condições estabelecidos neste edital e em seus anexos, abaixo relacionados:

Anexo I	Termo de Referência
Anexo II	Modelo de Carta Proposta
Anexo III	Modelo de Atestado de Capacidade Técnica
Anexo IV	Modelo de Declaração de pleno atendimento à habilitação
Anexo V	Modelo de Declarações – Exigências Legais
Anexo VI	Modelo de Declarações – Exigências Legais de Proteção de Dados
Anexo VII	Minuta de Contrato

- Início do Acolhimento de Propostas: **03/07/2024 às 10h00**
- Limite para Acolhimento das Propostas: **15/07/2024 até às 10h00**
- Data e hora da disputa: **15/07/2024 às 10h30**
- Endereço Eletrônico: www.portaldecompraspublicas.com.br
- Todas as referências de tempo no edital, no aviso e durante a Sessão Pública observarão obrigatoriamente o horário de Brasília – DF, e dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.
- Durante a sessão pública, a comunicação entre o Pregoeiro e as licitantes ocorrerá exclusivamente mediante troca de mensagens, no campo próprio do sistema eletrônico.
- Cabe à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócio diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

1 – RETIRADA DO EDITAL

1.1 – O edital contendo todas as normas, orientações, procedimentos, especificações, relação de documentos a serem apresentados, e demais informações indispensáveis à participação dos interessados na licitação, poderá ser retirado, gratuitamente, na página de Internet: www.sistemaocemg.coop.br/editais **ou** www.portaldecompraspublicas.com.br.

2 – CREDENCIAMENTO

2.1 – Somente poderão participar deste Pregão Eletrônico as licitantes devidamente credenciadas junto ao provedor do sistema, na página eletrônica www.portaldecompraspublicas.com.br.

2.2 – O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico.

2.3 – O uso da senha de acesso é de exclusiva responsabilidade da licitante, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao Sescoop / MG, responsabilidade por eventuais danos decorrentes de uso indevido de senha, ainda que por terceiros.

2.4 – O credenciamento da licitante junto ao provedor do sistema implica a presunção de sua capacidade técnica para realização das operações inerentes ao Pregão Eletrônico.

2.5 – O licitante deverá declarar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do edital.

2.6 – A declaração falsa relativa ao cumprimento dos requisitos de habilitação ou à conformidade da proposta sujeitará a licitante às sanções previstas neste edital.

2.7 – Caso haja divergências entre as disposições do edital e o Sistema do Portal de Compras Públicas, prevalecerá, sempre, as disposições do edital.

3 – CONDIÇÕES PARA PARTICIPAÇÃO NA LICITAÇÃO

3.1 – Poderão participar deste certame os interessados com objeto social compatível ao ramo pertinente ao objeto da presente licitação, que estejam legalmente estabelecidas e que satisfaçam às condições deste edital e de seus anexos.

3.2 – Não poderão participar desta licitação:

a) Empresas que se apresentarem sob a forma de consórcio, qualquer que seja sua forma de constituição;

b) Empresas que tenham sido sancionadas com a pena de suspensão do direito de licitar ou contratar com o SESCOOP – Unidade Nacional e Unidades Estaduais, durante o prazo da sanção aplicada;

c) Pessoa jurídica do mesmo grupo econômico ou com sócio(s) em comum de outra empresa que esteja participando desta licitação;

d) Pessoa jurídica que estiver sob processo de falência;

e) Empresas que tenham como sócio ou administrador, dirigente ou empregado do SESCOOP;

f) Sociedades estrangeiras não autorizadas a funcionar no Brasil;

g) Empresas declaradas inidôneas com fundamento na Lei Orgânica do TCU, podendo a consulta ao enquadramento, ser realizada pela licitante mediante acesso ao portal https://contas.tcu.gov.br/ords/f?p=INABILITADO:CERTIDAO:0; procedimento que também será adotado pela Comissão Permanente de Licitação. A empresa que, estando no rol das inidôneas, apresentar proposta na presente licitação será excluída do certame, a qualquer momento, não importando em que fase esteja o procedimento.

4 – ESCLARECIMENTOS / QUESTIONAMENTOS SOBRE O EDITAL

4.1 – Os interessados que necessitarem de quaisquer esclarecimentos / questionamentos sobre o edital, poderão solicitá-los ao Sescoop / MG, por escrito, até 3 (três) dias úteis antes da data fixada para a abertura da sessão pública, impreterivelmente, através do e-mail licitacoes@sistemaocemg.coop.br, mediante requerimento com identificação.

4.1.1 – Os pedidos de esclarecimentos / questionamentos deverão ser enviados no prazo estipulado no item 4.1 acima, considerando para tal o horário de funcionamento do Sescoop / MG, a saber, 08h30 as 17h30 horas de segunda a sexta-feira, exceto feriados legais.

4.1.2 – O título do e-mail deverá observar o modelo a seguir: **Esclarecimento / Questionamento referente ao processo licitatório Pregão Eletrônico 010/2024 (315855)**. No corpo do e-mail deverá ser expresso, além do questionamento / esclarecimento em si, os dados da licitante: Razão Social / CNPJ / Endereço / Telefone e Pessoa de Contato.

4.1.3 – É de responsabilidade da licitante, atestar que seu esclarecimento / questionamento foi efetivamente recebido pelo Pregoeiro / Comissão Permanente de Licitação do Sescoop / MG.

4.1.4 – Não será prestado nenhum esclarecimento, nem sanadas quaisquer dúvidas, cuja interpelação da licitante seja efetuada por telefone, ou mediante visita pessoal ao Sescoop / MG.

4.1.5 – Os pedidos de esclarecimentos / questionamentos encaminhados intempestivamente ou que não atendam ao disposto acima, serão desconsiderados pelo Pregoeiro / Comissão Permanente de Licitação, não sendo passíveis de resposta.

4.1.6 – Não sendo apresentadas solicitações de esclarecimentos / questionamentos dentro do prazo indicado no item 4.1 supra, pressupõe-se que os elementos aqui fornecidos são suficientemente claros e precisos para permitir a apresentação das propostas, não cabendo, portanto, às licitantes, direito a qualquer reclamação posterior.

4.1.7 – Os adendos, esclarecimentos, prorrogações e/ou retificações deste edital, serão publicados / disponibilizados aos interessados via Internet, no Portal do Sistema Ocemg, pelos endereços https://sistemaocemg.coop.br/editais/ e www.portaldecompraspublicas.com.br, no link correspondente a este edital.

4.1.8 – É responsabilidade **EXCLUSIVA** de cada licitante visitar diariamente os sítios acima indicados e verificar se o edital de seu interesse foi objeto de adendos, esclarecimentos, respostas aos questionamentos, prorrogações e/ou retificações, não cabendo qualquer responsabilidade ao Sescoop / MG, caso a licitante deixe de fazê-lo.

4.1.9 – Os esclarecimentos e os aditamentos divulgados passarão a fazer parte integrante do edital da licitação.

5 – REGISTRO INICIAL DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO (ANTES DA SESSÃO DE LANCES)

5.1 – A licitante deverá registrar sua proposta comercial, exclusivamente por meio do sistema eletrônico do Portal de Compras Públicas, disponível em www.portaldecompraspublicas.com.br, até a data e o horário agendados para o acolhimento da proposta, quando, então, encerrar-se-á automaticamente a fase de recebimento de proposta e documentos de habilitação, ficando certo e esclarecido que o envio da proposta por si só, implicará na plena aceitação, por parte da licitante, das condições estabelecidas neste edital e seus anexos.

5.2 – A licitante deverá registrar, de forma expressa no sistema eletrônico, **a descrição do objeto e o valor global ofertado para o lote único**, incluindo todos os impostos, tributos, taxas, fretes, entrega (embarque e desembarque), prestação dos serviços, mão de obra, garantia, despesas com transporte e alimentação dos profissionais (se for o caso), encargos fiscais e comerciais e quaisquer outros encargos necessários ao cumprimento total da obrigação, ficando certo e esclarecido que o Sescoop / MG não se responsabilizará por quaisquer ônus ou despesas adicionais.

5.3 – A licitante deverá declarar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do edital.

5.3.1 – A Declaração falsa relativa ao Pleno Atendimento aos Requisitos de Habilitação e Proposta sujeitará as licitantes às sanções previstas no item 14 do edital e nos artigos 39, 40 e 41 do Regulamento de Licitações e Contratos do SESCOOP.

5.3.2 – Ao declarar no campo do sistema eletrônico, a licitante assume que tomou conhecimento dos documentos constantes dos anexos IV (Modelo de Declaração de Pleno Atendimento à Habilitação), V (Declarações – Exigências Legais) e VI (Modelo de Declarações – Exigências Legais de Proteção de Dados) do edital, se comprometendo a cumpri-los integralmente, não cabendo qualquer alegação futura em contrário.

5.4 – **A licitante deverá encaminhar (anexar) proposta, concomitantemente com os documentos de habilitação exigidos neste edital,** exclusivamente por meio de campo próprio do sistema, até a data e o horário estabelecidos para acolhimento das propostas.

5.4.1 – Até o prazo para o encerramento do acolhimento das propostas, as licitantes poderão retirar ou substituir os documentos anteriormente apresentados.

5.4.2 – O sistema eletrônico resguardará o sigilo da proposta comercial e dos documentos de habilitação, não sendo possível a identificação da licitante pelo Pregoeiro ou demais empresas licitantes participantes.

5.4.3 – A proposta comercial e documentação de habilitação da licitante classificada provisoriamente em primeiro lugar, após o encerramento da etapa de lances, somente será disponibilizada para avaliação do Pregoeiro **após o encerramento da fase de disputa**.

6 – SESSÃO PÚBLICA DO PREGÃO, JULGAMENTO, NEGOCIAÇÃO, ACEITABILIDADE DA PROPOSTA E ANÁLISE DOS DOCUMENTOS DE HABILITAÇÃO

6.1 – O critério de julgamento das propostas será o **MENOR PREÇO GLOBAL**, desde que atendidas as especificações constantes deste edital e seus anexos, sendo desclassificadas as propostas que estiverem em desacordo com as especificações do anexo I deste edital.

6.2 – O Pregoeiro verificará as propostas apresentadas e desclassificará, motivadamente, aquelas que não estejam em conformidade com os requisitos estabelecidos neste edital.

6.3 – Somente as licitantes com propostas classificadas participarão da fase de lances.

6.4 – Aberta a **disputa de preços**, as licitantes classificadas poderão encaminhar lances sucessivos, exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do horário e valor consignados no registro de cada lance.

6.5 – A licitante somente poderá oferecer lance inferior ao último por ela ofertado e registrado no sistema.

6.6 – Durante o transcurso da sessão, as licitantes serão informadas, em tempo real, do valor do menor lance registrado, mantendo-se em sigilo a identificação da ofertante.

6.7 – Os lances apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade da licitante, não lhe cabendo o direito de pleitear qualquer alteração.

6.8 – Durante a fase de lances, o Pregoeiro poderá excluir, justificadamente, lance cujo valor seja manifestamente inexequível.

6.9 – Se ocorrer a desconexão do Pregoeiro no decorrer da etapa de lances e o sistema eletrônico permanecer acessível às licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

6.10 – No caso de a desconexão do Pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão será suspensa automaticamente e terá reinício somente após comunicação expressa aos participantes no sítio www.portaldecompraspublicas.com.br.

6.11 – Será adotado para o envio de lances no Pregão Eletrônico o modo de disputa **"ABERTO E FECHADO"**, em que as licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

> 6.11.1 – Modo de disputa **ABERTO E FECHADO**, ou seja, hipótese em que as licitantes deverão apresentar lances públicos e sucessivos, com lance final e fechado. Portanto, alertamos às licitantes que **é necessário anexar previamente a proposta e os documentos de habilitação**, exclusivamente por meio de campo próprio do sistema, após o registro de sua proposta no Sistema do Portal de Compras Públicas, disponível em www.portaldecompraspublicas.com.br.

6.12 – A etapa de lances da sessão pública terá duração inicial de 15 (quinze) minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até 10 (dez) minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

6.13 – Encerrado o prazo previsto no item anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez) por cento superior àquela, possam ofertar um lance final e fechado em até 5 (cinco) minutos, o que será sigiloso até o encerramento deste prazo.

6.14 – Não havendo, pelo menos, 3 (três) ofertas nas condições definidas neste item poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de 3 (três), oferecer um lance final e fechado até 5 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

6.15 – Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará os lances segundo a ordem crescente de valores.

6.16 – Não havendo lance final fechado e classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada para que os demais licitantes, até no máximo de 3 (três), na ordem de classificação, possam ofertar um lance final e fechado em até 5 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo, observando-se, após, o item anterior.

6.17 – Poderá o Pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atender as exigências de habilitação.

6.18 – O Pregoeiro poderá encaminhar contraproposta diretamente à licitante que tenha apresentado o lance mais vantajoso, observados o critério de julgamento e o valor estimado para a aquisição / contratação.

> 6.18.1 – A negociação será realizada por meio do sistema, podendo ser acompanhada pelas demais licitantes.

6.19 – Incumbirá à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

6.20 – **A licitante classificada provisoriamente em primeiro lugar** deverá encaminhar, **no prazo a ser indicado pelo Pregoeiro, sendo garantido o prazo mínimo de 2 (duas) horas**, contadas da solicitação do Pregoeiro, a proposta de preço adequada ao último lance, devidamente acompanhada dos documentos exigidos no item 6.21 abaixo, devendo o envio ocorrer, por meio de uma das seguintes opções:

a) Preferencialmente, por meio do Sistema do Portal de Compras Públicas, disponível em www.portaldecompraspublicas.com.br, no acesso identificado, sendo anexadas (cópias digitalizadas) ao sistema; ou

b) Para o e-mail licitacoes@sistemaocemg.coop.br.

6.20.1 – O percentual de desconto concedido pela empresa vencedora, após a rodada de lances, deverá ser aplicado proporcionalmente ao preço dos itens que compõem o lote único da licitação.

6.20.2 – O prazo estabelecido pelo Pregoeiro poderá ser prorrogado por deliberalidade, devidamente registrada no Chat ou por solicitação escrita e justificada da licitante, formulada antes de findo o prazo estabelecido, e formalmente aceita pelo Pregoeiro.

6.20.3 – De acordo com o Artigo 3º da Resolução nº 2056/2023 do SESCOOP, a licitação não será sigilosa, sendo acessíveis ao público os atos de seu procedimento, salvo quanto ao conteúdo das propostas até a respectiva abertura. Dessa forma, a documentação enviada pela licitante convocada pelo Pregoeiro, caso não seja anexada diretamente no Sistema do Portal de Compras Públicas, disponível em www.portaldecompraspublicas.com.br, será disponibilizada para vistas dos interessados no Portal Institucional do Sistema Ocemg, disponível em www.sistemaocemg.coop.br/editais.

6.21 – A proposta comercial da licitante classificada provisoriamente em primeiro lugar, **após o encerramento da etapa de lances**, deverá ser elaborada preferencialmente em papel timbrado da empresa, observando o modelo constante do anexo II deste edital, digitada em uma via, redigida em língua portuguesa, salvo quanto às expressões técnicas de uso corrente, devidamente assinada (de próprio punho ou de forma eletrônica) na última folha e rubricada nas demais folhas e anexos pelo representante legal / procurador, sem rasuras e emendas, entrelinhas ou ressalvas, atendendo, na forma e conteúdo, às condições fixadas neste Pregão, em especial:

a) Indicação da razão social, CNPJ, Inscrição Estadual e Municipal (se houver), endereço completo da empresa, telefone, pessoa de contato, e-mail e **dados bancários (nº da agência, nº da conta corrente e nome do banco)**;

b) Especificações claras, completas e detalhadas dos equipamentos e serviços ofertados, observando as informações contidas no anexo I deste edital, com indicação da(s) marca(s), modelo(s) ou referência(s) do(s) equipamento(s) ofertado(s);

b.1) A licitante deverá descrever exatamente os equipamentos e serviços que serão entregues, e não simplesmente transcrever as especificações constantes do anexo I do edital;

b.2) Fica vedado à licitante arrematante indicar, na proposta comercial final, marca distinta daquela informada na proposta comercial inicial, podendo ser desclassificada a empresa que descumprir esta obrigação;

b.3) Apresentação **obrigatória** de catálogos e/ou manuais e/ou descritivos técnicos e/ou materiais informativos e/ou folders dos equipamentos ofertados, contendo todas as especificações técnicas e características deles, que permitam atestar claramente a compatibilidade dos equipamentos ofertados com as especificações técnicas requeridas no anexo I do edital;

b.3.1) A licitante deverá indicar para cada item da especificação a página do catálogo e/ou manual e/ou descritivo técnico e/ou material informativo e/ou folder, onde é comprovado o atendimento dos requisitos exigidos no anexo I do edital;

b.3.2) Os catálogos e/ou manuais e/ou descritivos técnicos e/ou materiais informativos e/ou folders deverão referenciar a mesma marca e mesmo modelo dos equipamentos ofertados.

c) Indicação dos **preços unitários, totais e global**, cotados em Reais e expressos em até 2 (duas) casas decimais, incluindo todos os impostos, tributos, taxas, fretes, entrega (embarque e desembarque), prestação dos serviços, mão de obra, garantia, despesas com transporte e alimentação dos profissionais (se for o caso), encargos fiscais e comerciais e quaisquer outros encargos necessários ao cumprimento total da obrigação, ficando certo e esclarecido que o Sescoop / MG não se responsabilizará por quaisquer ônus ou despesas adicionais.

c.1) Em nenhuma hipótese o Sescoop / MG concederá reajustes de preços em razão de variação cambial. A licitante deverá, obrigatoriamente, prever e adotar as medidas de cautela para que eventuais variações na moeda estrangeira não impliquem em cancelamento da aquisição / contratação ou solicitação de reajuste de preços.

6.22 – Decorridos 60 (sessenta) dias da data do encerramento da fase de lances deste Pregão, sem convocação para realização do fornecimento / execução dos serviços, fica a licitante vencedora liberada do compromisso assumido.

6.22.1 – Se por motivo de força maior, a adjudicação não puder ocorrer dentro do período de validade da proposta, e caso persista o interesse do Sescoop / MG, este poderá solicitar a prorrogação da validade da proposta por igual prazo.

6.23 – O Pregoeiro examinará a proposta melhor classificada quanto à sua compatibilidade com as especificações técnicas do objeto. A aceitabilidade da proposta de preços classificada em primeiro lugar estará condicionada ao cumprimento dos requisitos elencados no item 6.21 deste edital.

6.23.1 – O Pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do Sescoop / MG ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão, podendo, para tanto, suspender a sessão pública, agendando nova data a ser comunicada via Chat do sistema eletrônico.

6.24 – Serão desclassificadas as propostas que:

a) Não atendam as condições contidas neste edital;

b) Apresentem preços com valores nulos ou zeros, simbólicos, inexequíveis, irrisórios ou incompatíveis com os preços praticados no mercado;

b.1) Considerar-se-á inexequível a proposta que não venha a ter demonstrada sua viabilidade por meio de documentação que comprove que os custos envolvidos no fornecimento / contratação são coerentes com os de mercado para o objeto deste **Pregão**, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração.

c) Apresentem cotação parcial e/ou vantagens baseadas nas ofertas das demais licitantes;

d) Não sejam feitas em moeda nacional;

e) Apresentem diferentes opções de preço para o mesmo item;

f) Deixem de atender às solicitações da Comissão ou da área técnica competente, quando da realização de diligência;

g) Deixem de assinar o Contrato de Fornecimento em até 3 (três) dias úteis, conforme item 14 do edital.

6.24.1 – Não se considerará como critério de avaliação das propostas, qualquer oferta de vantagem não prevista nesse edital, sem prejuízo de a licitante poder colocar à disposição do Sescoop / MG, outros fornecimentos e serviços e facilidades pertinentes a sua atividade-fim e que não importarão em qualquer remuneração / contraprestação por parte do Sescoop / MG.

6.25 – Em nenhuma hipótese poderá ser alterado o conteúdo da proposta apresentada, ressalvadas apenas aquelas destinadas a sanar evidentes erros materiais, a juízo exclusivo do Pregoeiro, puder ser sanável, sem a quebra de igualdade de tratamento oferecida a todos as licitantes.

6.26 – Não se desclassificarão as propostas pela simples ocorrência de vício que, a juízo exclusivo da Comissão, puder ser sanável, sem a quebra de igualdade de tratamento oferecida a todos as licitantes.

6.27 – Durante o prazo de julgamento, o Sescoop / MG poderá promover diligência destinada a esclarecer ou complementar a instrução do processo, podendo ainda solicitar de suas áreas internos, pareceres técnicos para apoio de sua decisão. A realização da diligência é uma prerrogativa exclusiva do Sescoop / MG, que poderá fazer uso das suas atribuições caso entenda que o erro, omissão, obscuridade ou dubiedade da proposta comercial e habilitação enquadra-se nos aspectos meramente formais.

6.27.1 – Caso quaisquer documentos relacionados no edital deixem de ser apresentados ou sejam apresentados com prazo de validade vencido, **poderá** o Pregoeiro / Comissão Permanente de Licitação, em observância aos princípios da competitividade, economicidade e razoabilidade, determinar prazo para que eles sejam apresentados e entregues, sob pena de desclassificação / inabilitação.

6.27.1.1 – Caso algum documento possa ser consultado, validado ou ainda extraído da internet, é prerrogativa do Pregoeiro e da Comissão Permanente de Licitação consultar os sites oficiais responsáveis pela emissão dos documentos, verificando se a licitante está regular no dia da abertura da sessão/licitação, mesmo que a documentação anexada no sistema eletrônico esteja vencida ou não tenha sido apresentada.

6.27.1.2 – A juntada posterior de documentos deverá comprovar situação pré-existente, ou seja, até a data da realização da sessão.

6.27.1.3 – O Sescoop / MG não se responsabilizará pela eventual indisponibilidade dos meios eletrônicos de informações, no momento da verificação da habilitação.

6.28 – Declarada encerrada a etapa competitiva, o Pregoeiro procederá à classificação definitiva das propostas, promovendo a classificação definitiva das propostas em ordem crescente de **MENOR PREÇO GLOBAL**.

6.29 – Análise da documentação de habilitação indicada no item 7 abaixo, apenas da empresa, cuja proposta tenha sido classificada em primeiro lugar.

6.30 – Sendo inabilitada a proponente cuja proposta tenha sido classificada em primeiro lugar, o Pregoeiro procederá com a análise da documentação de habilitação da proponente classificada em segundo lugar, e assim sucessivamente, se for o caso, até a habilitação de uma das licitantes.

6.31 – Proclamação da empresa vencedora do certame pelo critério de Menor Preço Global.

6.32 – Declarada a vencedora, qualquer licitante poderá manifestar imediata e motivadamente a intenção de recorrer, conforme previsto no item 9 do edital.

6.33 – Encaminhamento dos autos do processo à autoridade competente para adjudicação e homologação do certame, conforme previsto no item 10 do edital.

7 – HABILITAÇÃO

7.1 – Para habilitação nesta licitação, serão exigidos os seguintes documentos:

I – HABILITAÇÃO JURÍDICA

a) Ato Constitutivo ou Estatuto ou Contrato Social ou Cadastro de Empresário Individual, em vigor, devidamente registrado, em se tratando de sociedades comerciais e, no caso de sociedade por ações, acompanhado de documentos de eleição de seus administradores; ou Decreto de autorização, devidamente arquivado, em se tratando de Empresa ou Sociedade estrangeira em funcionamento no país e Ato de Registro ou Autorização para funcionamento, expedido pelo órgão competente, quando a atividade assim o exigir; ou Registro comercial, no caso de empresa individual;

a.1) O objeto social expresso no estatuto ou contrato social deverá especificar atividade pertinente e compatível com o objeto da presente licitação;

a.2) O contrato social primário deverá vir acompanhado das alterações contratuais subsequentes, relativas à alteração de razão social, capital social, composição societária e/ou objeto social; **podendo ser substituídos pela alteração contratual contendo a consolidação do contrato social**;

a.3) O contrato social e alterações poderão ser substituídos pela **Certidão Simplificada** emitida pela Junta Comercial do Estado sede da empresa licitante; ou pela **Certidão** emitida pelo Cartório de Registro de Pessoas Jurídicas, do Estado sede da empresa licitante.

b) Cópia da carteira de identidade e do CPF do(s) representante(s) legal(is) da empresa.

II – REGULARIDADE FISCAL

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) Prova de Regularidade para com a Fazenda Municipal (Certidão Negativa de Débitos – CND, mobiliária **ou** plena), expedida na sede ou domicílio da licitante;

c) Prova de Regularidade para com a Fazenda Estadual (Certidão Negativa de Débitos Tributários ou documento afim), expedida na sede ou domicílio da licitante;

d) Certificado de Regularidade do FGTS (CRF), expedido pela Caixa Econômica Federal, com a finalidade de comprovar a inexistência de débitos junto ao Fundo de Garantia por Tempo de Serviço – FGTS;

e) Certidão de Débitos Relativos a Créditos Tributários Federais e à Dívida Ativa da União, expedida pela Secretaria da Receita Federal do Brasil;

f) Prova de inexistência de débitos inadimplentes perante a Justiça do Trabalho, mediante a apresentação de certidão negativa (Certidão Negativa de Débitos Trabalhistas – CNDT).

III – QUALIFICAÇÃO TÉCNICA

a) No mínimo, **1 (UM) ATESTADO DE CAPACIDADE TÉCNICA**, emitido por pessoa jurídica de direito público ou privado, comprovando a empresa licitante já ter realizado o **fornecimento de solução de firewall do fabricante Sonicwall, incluindo o suporte técnico**, compatíveis com o objeto da licitação detalhado no anexo I (Termo de Referência), observando o modelo constante do anexo III deste edital;

a.1) O atestado deverá ser apresentado em papel timbrado do emitente e deverá conter, obrigatoriamente, as seguintes informações: identificação da pessoa jurídica e do responsável pela emissão da declaração; identificação da empresa licitante, quantitativos e descrição clara de cada item fornecido / serviços prestados;

a.2) A licitante será inabilitada na hipótese de não demonstrar estar capacitada ao fornecimento / execução dos serviços;

a.3) O não atendimento à capacidade técnica e produtiva implicará na inabilitação da respectiva licitante, sendo convocada a segunda colocada repetindo o procedimento, sucessivamente, até a apuração de uma que atenda as condições do edital;

a.4) Para fins de ratificação das informações contidas nos referidos Atestados, a Comissão poderá exigir, a título de diligência, cópias das notas fiscais e/ou contratos/pedidos referentes ao fornecimento / serviços descritos nos atestados.

b) Indicação do profissional que será responsável pela implementação da solução descrita no Termo de Referência constante do anexo I do edital e pela prestação da garantia de 90 (noventa) dias após a emissão do Termo de Recebimento Definitivo, mediante:

b.1) Comprovação de que o profissional possua no mínimo 01 (um) Certificado válido na solução do firewall ofertado, devendo o certificado ser emitido pelo fabricante da solução;

b.2) Comprovação de que o profissional indicado mantém vínculo com a empresa licitante, que poderá ocorrer através dos seguintes meios:

b.2.1) Instrumento de constituição da empresa, já exigido no item 7.1, inciso I, alínea “a” acima, caso o profissional seja sócio, proprietário ou dirigente da empresa; **OU**

b.2.2) Cópia da Carteira de Trabalho e Previdência Social (CTPS) **OU** da Ficha de Registro do Empregado, caso o profissional seja empregado da empresa;

b.2.3) Cópia do Contrato de Prestação de Serviços, em vigor na data agendada para realização da sessão pública de lances, firmado entre o profissional e a pessoa jurídica, caso o primeiro preste, para o segundo, serviços como profissional autônomo.

b.3) A documentação exigida nas alíneas “b.1” e “b.2” acima, caso não apresentados junto com a documentação de habilitação, poderão ser apresentados pela empresa após ela ser declarada vencedora da licitação, antes de realizada a homologação do certame;

b.4) O Sescoop / MG, por meio do fiscal do contrato, deverá ser previamente informado, da eventual substituição do profissional indicado. A empresa contratada deve encaminhar, por escrito, ao Sescoop / MG, no prazo de até 7 (sete) dias úteis a partir da saída do profissional, a justificativa da substituição dele, além do nome do substituto indicado, apresentando ainda toda a documentação exigida nas alínea**s** “b.1” e “b.2” acima.

b.4.1) A aprovação do nome do substituto pela empresa contratada estará subordinada à qualificação profissional igual ou superior à do profissional substituído e à expressa concordância do Sescoop / MG.

c) **DECLARAÇÃO** de menor, fato impeditivo de habilitação, conhecimento do instrumento convocatório, inexistência de impedimento e elaboração independente da proposta, conforme modelo constante no anexo V do edital;

d) **DECLARAÇÃO** como prova de atendimento as exigências legais de proteção de dados, conforme modelo contido no anexo VI do edital.

IV – QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

a) **CERTIDÃO NEGATIVA DE FALÊNCIA OU RECUPERAÇÃO JUDICIAL**, expedida pelo **distribuidor da sede da licitante** com data de emissão de, no máximo, 90 (noventa) dias de antecedência da realização da sessão pública.

7.2 – Os documentos deverão ser fornecidos, em 1 (uma) via de cada, em plena validade, em original ou extraídos da Internet ou cópia simples, **NÃO** podendo ser substituídos por qualquer tipo de protocolo.

7.3 – Os documentos/certidões exigidos para habilitação deverão ter validade na data de abertura da sessão pública no Sistema do Portal de Compras Públicas, disponível em www.portaldecompraspublicas.com.br. Na hipótese de não constar prazo de validade nos documentos/certidões apresentados, o **Sescoop / MG** aceitará como **válidas as expedidas até 90 (noventa) dias imediatamente anteriores a data de realização da Licitação.**

7.4 – A apresentação de certidões positivas, com efeitos de negativa, supre a exigência editalícia, não acarretando a inabilitação da licitante.

7.5 – Os documentos exigidos neste edital poderão ser apresentados mediante publicação em órgãos da imprensa oficial ou por qualquer processo de cópias simples, **não sendo necessária a autenticação deles.**

7.6 – Se a unidade da licitante participante do certame for a matriz, todos os documentos deverão estar em nome da matriz, e se a licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, forem emitidos somente em nome da matriz.

7.7 – Os documentos eletrônicos produzidos com a utilização de processo de certificação disponibilizada pela ICP-Brasil, nos termos do art. 10, § 1º e § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, serão recebidos e presumidos verdadeiros em relação aos signatários, dispensando-se o envio de documentos originais e cópias autenticadas em papel.

8 – RESULTADO

8.1 – Se a proposta de preços não for aceitável, ou se a licitante **não atender às exigências de habilitação**, o Pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda a este edital.

8.2 – Constatado o atendimento às exigências fixadas neste edital, a licitante será declarada vencedora.

9 – RECURSOS ADMINISTRATIVOS

9.1 – O interesse da licitante em interpor recurso deverá ser manifestado, imediata e motivadamente e, por meio do sistema eletrônico, no prazo máximo de 30 (trinta) minutos após a declaração do vencedor, quando lhe será concedido o prazo de 2 (dois) dias úteis para apresentação das razões do recurso.

9.2 – A licitante que puder vir a ter a sua situação efetivamente prejudicada em razão de recurso interposto poderá sobre ele se manifestar no mesmo prazo recursal, que começará a fluir, a contar da ciência da interposição do recurso.

9.3 – As razões e contrarrazões de recurso deverão ser enviadas **exclusivamente** por meio do Portal de Compras Públicas, disponível em www.portaldecompraspublicas.com.br, no link correspondente a este edital.

9.3.1 O recurso deverá ser dirigido ao Superintendente do Sescoop / MG, por intermédio do Pregoeiro / Comissão Permanente de Licitação, nos dias e horários de funcionamento da entidade, a saber, 08h30 as 17h30, de segunda a sexta feira, exceto feriados legais.

9.3.2 Eventuais recursos poderão ser respondidos/contrarrazoados pelas licitantes interessadas, em prazo idêntico para a interposição do recurso, 2 (dois) dias úteis, a contar da ciência da interposição do recurso, cujo procedimento observará o estabelecido no item 9.3.

9.4 – A falta de manifestação imediata e motivada da licitante importará a decadência do direito de recurso e a adjudicação do objeto da licitação pela autoridade competente à vencedora.

9.5 – O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

9.6 – Os recursos administrativos terão efeito suspensivo e serão julgados pelo Superintendente do Sescoop / MG ou por quem este delegar competência.

10 – HOMOLOGAÇÃO E ADJUDICAÇÃO

10.1 – Após comunicação do resultado, caso não tenha sido interposto recurso ou se já decididos os porventura interpostos, o Pregoeiro remeterá o processo à Superintendência do Sescoop / MG para homologação e autorização de adjudicação do objeto à licitante vencedora.

10.2 – A Superintendência do Sescoop / MG poderá cancelar a presente licitação, antes de assinado o Contrato de Fornecimento, por motivo justificado, conforme previsto no Artigo 62, do Regulamento de Licitações e Contratos do SESCOOP.

11 – CONTRATO

11.1 – Tão logo seja homologada a decisão, a licitante vencedora receberá por e-mail, um link para acesso à plataforma denominada TOTVS Assinatura Eletrônica, para assinatura do Contrato, que deverá ser atendido em todos os seus termos pela licitante vencedora, que terá o prazo máximo de 3 (três) dias úteis para assinatura.

11.1.1 – A recusa injustificada em assinar o Contrato de Fornecimento, dentro do prazo fixado, caracterizará o descumprimento total da obrigação assumida e poderá acarretar à licitante vencedora a perda do direito ao fornecimento, bem como as penalidades previstas no item 14 abaixo.

11.1.2 – O Sescoop / MG terá a prerrogativa de enviar o Contrato de Fornecimento por e-mail ou notificar a licitante vencedora para que compareça na Rua Ceará, nº 771, bairro Santa Efigênia, CEP 30.150-312, em Belo Horizonte – MG, para assinatura do documento de forma física, observando o mesmo prazo indicado no item 11.1 acima.

12 – PRAZO DE VIGÊNCIA DO CONTRATO / REAJUSTE

12.1 – O prazo de vigência do Contrato será de 7 (meses) meses, compreendo a entrega dos equipamentos e softwares, realização dos serviços e prestação da garantia por parte da empresa contratada, iniciando-se na data de sua assinatura, podendo ser prorrogado, a critério do Sescoop / MG, mediante elaboração de termo aditivo.

12.2 – Os equipamentos e softwares deverão ser entregues no prazo máximo de 45 (quarenta e cinco) dias úteis após a assinatura do contrato, e os serviços realizados, inclusive documentação, no prazo máximo de 30 (trinta) dias úteis após entrega dos equipamentos / softwares, diretamente na Sede do Sescoop / MG, localizada na Rua Ceará, nº 771, Bairro Santa Efigênia, CEP 30150-311, em Belo Horizonte/MG.

12.2.1 – Previamente à entrega / execução dos serviços, a empresa contratada deverá obrigatoriamente, efetuar contato com a Gerência de Tecnologia da Informação (GETIN) do Sescoop / MG, cujos dados para contato serão informados quando da assinatura do contrato, visando acertar os detalhes da entrega / execução dos serviços e demais informações que se fizerem necessárias.

12.2.2 – Por ocasião da entrega dos equipamentos / softwares e realização dos serviços, a empresa contratada deverá observar rigorosamente as especificações técnicas que deverão corresponder àquelas descritas no anexo I do edital e demais disposições do contrato. A não obediência a este quesito acarretará a devolução sumária dos equipamentos / serviços e a aplicação das penalidades cabíveis.

12.2.2.1 – Os equipamentos entregues deverão ser novos, de 1º uso e em linha de produção mais recente, igual ou superior tecnologicamente, à época de aquisição, não sendo aceito equipamentos utilizados em exposições, feiras ou eventos promocionais.

12.2.2.2 – Os equipamentos entregues em desconformidade com as especificações contratadas serão passíveis de devolução à empresa contratada, cabendo a esta todo e quaisquer ônus decorrentes, inclusive, se for o caso, o cancelamento de Nota Fiscal, mesmo que emitida em mês anterior, ficando entendido que a entrega de equipamentos em desconformidade é considerada falta grave, podendo ensejar a aplicação das penalidades cabíveis.

12.2.2.3 – Os equipamentos entregues estarão sujeitos à inspeção pelo Sescoop / MG, que poderá rejeitá-los (no todo ou em parte) se considerá-los defeituosos ou divergentes com relação às especificações. Os equipamentos rejeitados serão restituídos à empresa contratada, por sua conta e risco. Todas as despesas com desembalagem, reembalagem e devolução dos equipamentos serão debitadas à empresa contratada.

12.2.3 – A realização dos serviços deverá ser efetuada por técnicos da empresa contratada / fabricante, sendo acompanhada por técnicos indicados pelo Sescoop / MG, no local no item 12.2 acima.

12.2.4 – O atraso na entrega dos equipamentos / softwares e execução dos serviços ensejará a aplicação da multa, conforme previsto neste edital.

12.3 – Eventuais solicitações de prorrogação do prazo de entrega somente **serão analisadas** se atenderem às seguintes condições:

a) O pedido for encaminhado à Comissão Permanente de Licitação, sendo desconsiderados para efeito de isenção de multa, os pedidos encaminhados diretamente à outras Gerências do Sescoop / MG, mesmo que deferidos;

b) O pedido for enviado à Comissão Permanente de Licitação antes de expirada a data de entrega contratada. Vencida a data de entrega não haverá isenção de multas;

c) O eventual atraso decorrer de caso fortuito ou força maior, assim entendidas as circunstâncias absolutamente imprevisíveis e insuperáveis por parte da empresa contratada. A falta de programação, ou acordo, ou entendimento entre a empresa contratada e seus fornecedores/fabricantes não são motivos para prorrogação da data.

12.4 – O pedido de prorrogação será analisado pela Comissão Permanente de Licitação, podendo ser deferido ou indeferido, formalmente, ficando certo e esclarecido que o indeferimento não desobriga a empresa contratada de entregar os equipamentos, sujeitando-se a mesma, neste caso, às penalidades cabíveis. A negativa de entrega, em face do indeferimento, será considerada falta grave, podendo ensejar a suspensão do direito de licitar e contratar com o Sescoop, nos termos deste edital.

13 – FATURAMENTO E FORMA DE PAGAMENTO

13.1 – O faturamento deverá ocorrer 100% (cem por cento) após a realização da entrega dos equipamentos / softwares, bem como realização dos serviços e o pagamento será efetuado no prazo máximo de 28 (vinte oito) dias corridos, mediante a apresentação da Nota Fiscal / Fatura pela empresa contratada, devidamente aprovada pela Gerência de Licitações e Compras do Sescoop / MG, sem prejuízo de eventuais multas por atraso.

13.1.1 – A nota fiscal / fatura deverá ser encaminhada para o e-mail notasfiscais@sistemaocemg.coop.br contendo os dados bancários para pagamento, que será realizado preferencialmente via depósito em conta.

13.1.2 – No caso de emissão de Nota Fiscal na forma “eletrônica”, a empresa contratada fica obrigada a enviar juntamente com o documento o arquivo eletrônico denominado “XML” para fins de conferência e fechamento junto a receita estadual. A Nota Fiscal ficará retida para pagamento, até o envio do presente arquivo.

13.1.3 – Não será aceita Nota Fiscal / Fatura de serviços emitida entre o dia 21 e 31 de determinado mês. A ocorrência de tal fato implicará na devolução sumária, ficando a empresa contratada obrigada a substituir o documento.

13.1.4 – O Sescoop / MG poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela empresa contratada, nos termos deste Pregão.

13.1.5 – No caso de incorreção na Nota Fiscal, esta será restituída à empresa contratada para as correções solicitadas. O prazo de pagamento será contado a partir da data da regularização do documento fiscal, não respondendo o Sescoop / MG por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.

13.1.6 – Caso os equipamentos e serviços constantes da Nota Fiscal / Fatura estejam em desacordo com os equipamentos entregues / serviços executados, ela não será liberada para pagamento, até a correção do fato. Caberá à empresa contratada a solução do problema para aprovação dos equipamentos / serviços pelo Sescoop / MG e liberação do pagamento.

13.1.7 – O Sescoop / MG fará a retenção dos impostos de acordo com a legislação vigente, caso aplicável.

13.1.8 – Retenção de Imposto Sobre Serviço de Qualquer Natureza (ISSQN): de acordo com a Legislação, as Microempresas ou as Empresas de Pequeno Porte, optantes pelo Simples Nacional, que não informarem, a alíquota de retenção nos documentos fiscais, será aplicada a alíquota de 5% (cinco por cento).

13.2 – A aceitação dos equipamentos / serviços não exime a empresa contratada da responsabilidade quanto à qualidade dos mesmos e não invalida qualquer reclamação posterior do Sescoop / MG.

13.3 – A Nota Fiscal / Fatura deverá ser emitida pela empresa contratada, obrigatoriamente com o número de inscrição do CNPJ apresentado no processo licitatório, não se admitindo Nota Fiscal / Fatura emitida com outro CNPJ, mesmo de filiais ou da matriz da empresa contratada.

13.4 – Salvo autorização expressa e por escrito do Sescoop / MG, é vedado à empresa contratada, seja por qual motivo for, o desconto ou negociação de duplicatas, faturas e afins em instituições financeiras, relativamente a parcelas de pagamento vinculadas ao fornecimento do objeto deste edital / Contrato de Fornecimento.

14 – PENALIDADES

14.1 – A prática de atos ilícitos, em quaisquer das fases do procedimento licitatório, o descumprimento de prazos e condições do edital, implicarão na aplicação das penalidades previstas nos artigos 39, 40 e 41 do Regulamento de Licitações e Contratos do SESCOOP, sem prejuízo das demais sanções previstas em Lei, garantida a defesa prévia.

14.2 – A recusa injustificada em assinar o Contrato de Fornecimento, dentro do prazo fixado, caracterizará o descumprimento total da obrigação assumida e poderá acarretar à licitante as seguintes penalidades:

a) Perda do direito ao fornecimento / contratação;

b) Multa de 10% (dez por cento) do valor total estimado da aquisição / contratação;

c) Suspensão do direito de licitar ou contratar com o Sescoop / MG, por prazo não superior a 5 (cinco) anos.

14.3 – O não fornecimento / inexecução total ou parcial injustificado, o fornecimento / inexecução deficiente, irregular ou inadequada do objeto licitatório, pela empresa contratada, assim como o descumprimento dos prazos e condições estipulados e, sem prejuízo delas, implicarão nas penalidades abaixo mencionadas:

a) Será cobrada multa por atraso na ativação das licenças, no percentual de 0,5% (meio por cento) ao dia, referente a parcela em atraso, limitada a 10% (dez por cento) do valor total do Contrato de Fornecimento;

b) Advertência;

c) Rescisão do Contrato de Fornecimento;

d) Suspensão do direito de licitar ou contratar com o Sescoop / MG, nos termos da alínea “c” do item 14.2 supra.

14.4 – Ocorrendo aplicação de multa, esta será descontada sobre o valor da nota fiscal/fatura ou dos créditos a que a empresa contratada fizer "jus", no ato do pagamento, ou recolhidas diretamente à tesouraria do Sescoop / MG, ou ainda, quando for o caso, cobrada judicialmente.

14.5 – Para aplicação das penalidades aqui previstas, com exceção à multa indicada na alínea "a" do item 14.3 supra, que será aplicada de maneira automática, a empresa contratada será notificada para apresentação de defesa prévia, no prazo de 5 (cinco) dias úteis, contados da notificação.

14.6 – As penalidades previstas são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, sem prejuízo de outras medidas cabíveis, tal como o cancelamento previsto na alínea "c" do item 14.3 acima.

14.7 – Além das hipóteses indicadas acima, as licitantes / empresa contratada, perderão o direito de licitar e contratar com o Sescoop / MG, nas seguintes hipóteses:

a) Apresentar declaração ou documentação falsa exigida para o certame/fornecimento/contratação ou prestar declaração falsa durante a licitação ou a execução do contrato;

b) Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

c) Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

d) Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

e) Praticar ato lesivo previsto no artigo 5º da Lei nº 12.846, de 1º de agosto de 2013.

15 – FONTE DE RECURSOS E ESTIMATIVA DE PREÇOS

15.1 – As despesas inerentes à execução do objeto da presente licitação correrão por conta de recursos próprios do Sescoop / MG, consignados também em seu orçamento.

15.2 – A estimativa da licitação faz parte da fase interna do processo licitatório, sendo obtida através de pesquisa de mercado, devendo ser utilizada para verificação e aceitabilidade das propostas apresentadas.

> 15.2.1 – As propostas com preços manifestamente inexequíveis ou excessivamente altos, assim considerados aqueles que não venham a ter demonstrada sua viabilidade através de documentação que comprove que os custos dos insumos são coerentes com os preços praticados no mercado, serão desclassificadas após avaliação da Comissão Permanente de Licitação.

15.3 – O Sescoop / MG, de modo a incentivar a disputa de preços entre os licitantes, adota como política interna a **não** divulgação dos valores estimados de suas aquisições / contratações, em especial as que são conduzidas na modalidade de Pregão Eletrônico, em que se espera a competividade com ampla disputa de lances.

16 – DISPOSIÇÕES GERAIS

16.1 – Fica assegurado ao Sescoop / MG o direito de alterar as condições deste edital de acordo com seu interesse, desde que seja feita divulgação pela mesma forma que se deu o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar, substancialmente, a formulação das propostas.

16.2 – Na contagem dos prazos estabelecidos no Regulamento de Licitações e Contratos do SESCOOP, excluir-se-á o dia do início e incluir-se-á o do vencimento, e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário. Para fins deste item, esclarecemos que os prazos somente se iniciam e vencem em dia funcionamento do Sescoop / MG.

16.3 – As licitantes são responsáveis, em qualquer época, pela fidelidade e veracidade das informações dos documentos apresentados.

16.4 – Os casos omissos desta licitação serão resolvidos pelo Pregoeiro e equipe de apoio do Sescoop / MG, com aplicação do Regulamento de Licitações e Contratos do SESCOOP.

16.5 – O Sescoop / MG poderá introduzir acréscimos que se fizerem necessários, em até 50% (cinquenta por cento) do valor inicial do Contrato de Fornecimento, conforme lhe faculta o artigo 38 do Regulamento de Licitações e Contratos do SESCOOP, mediante elaboração e assinatura de termo aditivo.

16.5.1 – Eventuais supressões serão previamente acordadas entre as partes, sem existência de limitação.

16.6 – O Sescoop / MG poderá cancelar ou revogar a presente licitação por qualquer motivo justificável, desde que tal medida seja adotada antes de assinado o Contrato de Fornecimento, não cabendo às licitantes qualquer direito de reivindicação, indenização ou contestação, ficando certo e esclarecido que o cancelamento ou a revogação encontram-se no âmbito do poder discricionário da Entidade promotora da licitação.

16.7 – Todos os documentos relacionados a presente licitação, desde que emitidos pela Comissão Permanente de Licitação, são considerados complementares entre si, de modo que qualquer informação ou detalhe, mencionado em um documento e omitido em outros, será considerado especificado e válido.

16.8 – Encontra-se disponível para acesso das licitantes, em sistemaocemg.coop.br-portal-de-privacidade-politica-de-privacidade-sescoop-mg.pdf, a Política de Proteção de Dados Pessoais do Sescoop / MG.

16.9 – O Foro da Comarca de Belo Horizonte, Minas Gerais, será o competente para dirimir as questões oriundas desta licitação e da relação jurídica dela decorrente.

Belo Horizonte, 02 de julho de 2024.

Misael Gomes da Silva
Pregoeiro

Robert Martins Santos
Presidente da Comissão Permanente de Licitação
Autoridade Competente

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO:

1.1 – Contratação de empresa especializada para fornecimento de software, hardware, serviço de instalação, migração, configuração e otimização para solução de firewall, modelo SonicWall Gen 7 NSa 2700, com alta disponibilidade (HA – High Availability), contendo Advanced Protection Security Suite, pelo período de 36 (trinta e seis) meses, incluindo o suporte técnico do fabricante por igual período, para atender as necessidades do Sescoop / MG.

2. JUSTIFICATIVA:

2.1 – Este Termo de Referência tem como objetivo definir as diretrizes e requisitos para a aquisição de uma solução de firewall para o Sescoop / MG. Diante da crescente importância da segurança da informação no cenário atual, o Sescoop / MG está empenhado em reforçar seus mecanismos de proteção, assegurando a integridade, confidencialidade e disponibilidade de seus sistemas e dados.

2.2 – No contexto de ameaças cibernéticas em constante evolução, é vital que o Sescoop / MG implemente medidas robustas para proteger suas informações sensíveis e garantir o funcionamento adequado de suas operações. Nesse sentido, a aquisição/atualização de uma solução de firewall moderna e eficaz é essencial para mitigar riscos, prevenir incidentes de segurança e assegurar a continuidade das atividades institucionais.

2.3 – O firewall desempenha um papel fundamental na proteção dos ativos digitais, servindo como uma barreira de defesa que controla o fluxo de dados entre redes, monitora e filtra o tráfego com base em regras predefinidas. Esta solução tecnológica proporciona uma camada adicional de proteção, permitindo a implementação de políticas de segurança rigorosas, a detecção de atividades suspeitas e a prevenção de acessos não autorizados.

2.4 – A seleção adequada de uma solução de firewall é crucial para garantir que o Sescoop / MG esteja alinhado às melhores práticas de segurança da informação, buscando atender às normas e regulamentações vigentes. Ao adotar uma abordagem abrangente e proativa, reafirma seu compromisso em proteger os dados e a privacidade, promovendo a confiança e a transparência em suas operações.

2.5 – Com o objetivo de cumprir o princípio da padronização e assegurar a compatibilidade das especificações técnicas e de desempenho, consideramos as condições de manutenção, assistência técnica e garantia oferecidas. Dessa forma, optamos por renovar a solução atualmente em uso, o SonicWall NSA, em sua versão atualizada, modelo NSa 2700. Esta decisão é fundamentada na reputação do software como uma das principais ferramentas de segurança do mercado, cujo desempenho tem se mostrado excelente e atendido de forma satisfatória às necessidades do Sescoop / MG.

2.6 – A ferramenta, já em uso há mais de 5 (cinco) anos, tem demonstrado estabilidade no ambiente da entidade e nosso corpo técnico já possui expertise no funcionamento da solução. Desde então, a solução sempre nos atendeu de maneira eficaz e eficiente. Por se tratar de uma renovação, os custos são mais vantajosos do que à aquisição de novas ferramentas eliminando o risco de incompatibilidade, bem como a possibilidade de parada sistêmica do sistema informatizado até seu restabelecimento, o que poderia ocasionar perdas financeiras significativas à instituição.

2.7 – O SonicWall NSA tem se mostrado uma solução robusta, protegendo nossa infraestrutura de TI contra ciberataques. Com essa ferramenta, os ataques virtuais sofridos não surtiram efeito, reforçando sua eficácia. Além disso, a renovação dessa solução representa economicidade, pois evita gastos com a aquisição e implementação de novas ferramentas, treinamento técnico e custo da curva de aprendizagem. Isso demonstra o compromisso e a eficiência do Sescoop / MG com a gestão responsável dos recursos.

2.8 – Os serviços proporcionados pelo uso de recursos computacionais são fundamentais para o Sescoop / MG, pois são críticos para a realização de seus objetivos estratégicos e para o cumprimento de sua missão junto às cooperativas. A ausência de uma ferramenta eficiente, capaz de remediar, neutralizar e/ou reduzir ataques virtuais em um tempo aceitável, pode expor a organização a desgastes operacionais, perda irreversível de informações e obsolescência tecnológica, além de comprometer a LGPD. Portanto, a adoção de soluções robustas e confiáveis, como o SonicWall NSA 2700, é essencial para garantir a segurança, eficiência e economicidade de nossas operações.

3. SERVIÇO

3.1 – A empresa contratada deverá executar todo o serviço necessário a plena operacionalização da solução ofertada, devendo obrigatoriamente incluir todos os serviços abaixo:

a) Reunião de Quick off do projeto;
b) Planejamento detalhado dos procedimentos a serem executados;
c) Apresentação ao cliente do cronograma e processos para aprovação;
d) Instalação física dos componentes de hardware fornecidos no rack do Sescoop / MG;
e) Interligação dos componentes de hardware fornecidos a rede/links do Sescoop / MG de forma redundante;
f) Prestar auxílio em qualquer configuração de rede necessária a instalação da solução;
g) Instalação do licenciamento necessário;
h) Atualização de firmware dos componentes de hardware fornecidos;
i) Configuração da alta disponibilidade do hardware fornecido;
j) Levantamento de todas as regras de firewall, filtros de conteúdo, IPS,IDS, anti-malware e demais proteções existentes nos firewalls antigos do Sescoop / MG;
k) Migração, ajustes e otimização de todas as regras de firewall e demais configurações de controle e segurança aos novos firewalls;
l) Criar ou ajustar novas políticas de segurança conforme definição do Sescoop / MG;
m) Criar ou ajustar novas regras de firewall conforme definição do Sescoop / MG;
n) Implementar, criar ou ajustar um ambiente seguro de Captive Portal corporativo seguindo as melhores práticas;
o) Configurar e atualizar os relatórios existentes no software Global Management System (GMS) atualmente instalado e licenciado no Sescoop / MG;
p) Proceder a testes de funcionalidade antes da entrada em produção;
q) Proceder o acompanhamento da entrada em produção de forma presencial ou remota, dependendo da criticidade no ambiente do Sescoop / MG, com no mínimo 7 dias de acompanhamento;
r) Proceder aos ajustes necessários para solução dos problemas apresentados durante a entrada em produção;
s) Proceder a documentação completa contendo o passo a passo da nova solução instalada;
t) Proceder a um treinamento hands-on de no mínimo 8 horas sobre a solução instalada, incluindo o gerenciamento básico dos recursos migrados/ativos da solução de firewall, relatórios;
u) A empresa contratada deverá obrigatoriamente registar os novos equipamentos na conta institucional do Sescoop / MG no site MySonicWall (https://www.mysonicwall.com/).

3.2 – Quaisquer outros serviços necessários ao pleno funcionamento da solução deverão ser executados pela empresa contratada mesmo que não estejam listados acima.

3.3 – Todos os serviços devem ser executados de forma a não gerar paradas no ambiente de produção do Sescoop / MG durante o horário comercial. Serviços com risco ou necessidade de parada do ambiente de produção, deverão obrigatoriamente ser executados fora de horário comercial.

3.4 – A empresa contratada deve estar ciente que o Sescoop / MG não executará serviços que só podem ser realizados presencialmente. De forma explicita ficam definidos que os serviços de instalação física, serão obrigatoriamente executados de forma presencial no endereço do Sescoop / MG e não permitem negociação de atendimento remoto pela empresa contratada.

3.5 – A empresa contratada deverá fornecer 04 (quatro) cabos de conexão direta DAC SFP 10G 1,0 Metro.

4. ESPECIFICAÇÃO TÉCNICA DA FERRAMENTA FIREWALL:

PRODUTO SOLUÇÃO DE FIREWALL	LOTE ÚNICO / QUANTIDADE
SonicWall Gen 7 NSa 2700 appliances 01 (ou superior do mesmo fabricante).	**01**
SonicWall Gen 7 NSa 2700 appliances 02 (HA – High Availability).	
Software Advanced Protection Security Suite.	
Garantia do fornecedor (3 anos).	
Suporte técnico do fornecedor (3 anos).	
Serviço de instalação/migração, configuração e otimização.	
Fornecimento de 04 Cabos de Conexão Direta DAC SFP 10G 1,0 Metro.	**04**

4.1 – REQUISITOS MÍNIMOS

4.1.1 – O equipamento deve ser obrigatoriamente novo, em linha de montagem e de primeiro uso, podendo, a critério da empresa contratada, utilizar ou não o sistema de benefícios SonicWall Secure Upgrade appliance.

4.1.2 – Fornecimento e instalação do software de segurança Advanced Protection Security Suite com todas suas features habilitadas durante 3 (três) anos em ambos os appliances fornecidos na solução com alta disponibilidade (HA).

4.1.3 – Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 3.0 Gbps ou superior.

4.1.4 – Desempenho em modo de Inspeção (descriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 800 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.

4.1.5 – Desempenho mínimo de 3.4 Gbps de IPS.

4.1.6 – Suporte mínimo de 1.500.000 conexões simultâneas/concorrentes no modo SPI.

4.1.7 – Suporte mínimo de 21.000 novas conexões por segundo.

4.1.8 – Deve possuir armazenamento interno de no mínimo 64 GB e suportar expansão de armazenamento interno para até 256Gb.

4.1.9 – Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.

4.1.10 – Deve possuir 16 interfaces 1 GbE padrão RJ-45.

4.1.11 – Deve possuir 3 interfaces 10GbE SFP+.

4.1.12 – Deve possuir 1interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.

4.1.13 – Deve possuir 2 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

4.1.14 – A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1000 usuários simultâneos.

4.1.15 – A VPN SSL deve ser licenciada para, no mínimo, 02 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 500 usuários simultâneos.

4.1.16 – Deve suportar 2000 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

4.1.17 – Deve suportar, no mínimo, 2.1Gbps de desempenho de VPN IPSEC.

4.1.18 – Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao Sescoop / MG o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, a licitante será considerada inabilitada. Todos os custos oriundos do teste de bancada serão custeados pela licitante vencedora do certame.

4.1.19 – O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.

4.1.20 – O Equipamento deverá ser homologado pela ANATEL.

4.1.21 – Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

4.1.22 – O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no mínimo 36 (trinta e seis) meses.

4.1.23 – É imprescindível que a solução não possua um limite de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

4.2 – CARACTERÍSTICAS GERAIS DOS FIREWALLS FÍSICOS

4.2.1 – Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

4.2.2 – Para proteção do ambiente contra-ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.

4.2.3 – A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

4.2.4 – Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade.

4.2.5 – 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.

4.2.6 – Os firewalls devem ser entregues com licenciamento válido para, no mínimo, 36 meses, incluindo garantia e suporte.

4.2.7 – Deverá ser fornecido suporte técnico com a fabricante do produto durante 36 meses no mínimo.

4.3 – CARACTERÍSTICAS DIVERSAS

4.3.1 – Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.

4.3.2 – 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 (NAT-T) e NAT dentro do tunel IPSec.

4.3.3 – Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

4.3.4 – Deve possuir proteção anti-spoofing.

4.3.5 – Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

4.3.6 – Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.

4.3.7 – Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação.

4.3.8 – A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.

4.3.9 – Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

4.3.9.1 – Latência;

4.3.9.2 – Jitter;

4.3.9.3 – Perda de pacotes.

4.3.10 – O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal logico.

4.3.11 – A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.

4.3.12 – A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

4.3.13 – Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

4.3.14 – Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

4.3.15 – Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

4.3.16 – 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 via VPN.

4.3.17 – Deve suportar DHCP relay.

4.3.18 – 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 serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

4.3.19 – Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (física e virtual) ou zona de segurança.

4.3.20 – Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.

4.3.21 – Deve ter suporte à proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

4.3.22 – Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.

4.3.23 – Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood etc.

4.3.24 – Detectar e bloquear a origem de portscans.

4.3.25 – Deve permitir o bloqueio de ataques.

4.3.26 – Deve permitir o bloqueio de exploits conhecidos.

4.3.27 – O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP e SMTP.

4.3.28 – Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser descriptografado de forma transparente à aplicação.

4.3.29 – Implementar DSCP (Differentiated Services Code Points).

4.3.30 – Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, 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 da rede.

4.3.31 – Implementar controle e gerenciamento de banda para a tecnologia VoIP(Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

4.3.32 – Implementar mecanismo de sincronismo de horário através do protocolo NTP.

4.3.33 – Possuir suporte ao protocolo SNMP versões 2 e 3.

4.3.34 – Possuir suporte a log via syslog.

4.3.35 – Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

4.3.36 – O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período, e baseado em normas nacionais e internacionais de segurança da informação.

4.3.37 – Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes.

4.3.38 – 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 e-mail.

4.3.39 – Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

4.3.40 – Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3.

4.3.41 – Deve permitir a funcionalidade de ARP bridging.

4.3.42 – Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm".

4.4 – CARACTERÍSTICAS DE VPN

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

4.4.2 – Suportar algoritmos de criptografia 3DES, AES 128 e AES 256.

4.4.3 – Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

4.4.4 – Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.

4.4.5 – Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.

4.4.6 – Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.

4.4.7 – A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

4.4.8 – Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.

4.4.9 – Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

4.4.10 – Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.

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

4.4.12 – Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

4.4.13 – Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

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

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

4.4.16 – Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

4.5 – ALTA DISPONIBILIDADE (HA)

4.5.1 – Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. 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.

4.5.2 – A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Passivo, com as implementações de Failover.

4.5.3 – Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.

4.5.4 – A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.

4.5.5 – A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.

4.5.6 – A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

4.5.7 – A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.

4.5.8 – A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.

4.5.9 – A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que haja perda das conexões de VPN, FTP, Oracle SQL*NET, RSTP, Real Audio, VPN Client, Dynamic Arp Objects, Informações de DHCP Server, Multicast , IGMP, Usuários ativos, RIP e OSPF.

4.6 – CONTROLE DE AMEAÇAS

4.6.1 – Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.

4.6.2 – A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

4.6.3 – Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

4.6.4 – Implementar funcionalidade de detecção e bloqueio de “call-backs”.

4.6.5 – A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

4.6.6 – A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.

4.6.7 – Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

4.6.8 – Implementar interface CLI segura através do protocolo SSH.

4.6.9 – Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

4.6.10 – A solução deve permitir criar regras de exceção de acordo com a proteção.

4.6.11 – Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

4.6.12 – Permitir o bloqueio de malwares (vírus, worms, spyware etc.).

4.6.13 – A solução deve ser capaz de proteger contra-ataques a DNS.

4.6.14 – A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

4.6.15 – A solução deve ser capaz de prevenir acesso a websites maliciosos.

4.6.16 – A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

4.6.17 – A solução deverá receber atualizações de um serviço baseado em cloud.

4.6.18 – A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

4.6.19 – A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

4.6.20 –A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade

4.6.21 – A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown.

4.6.22 – A solução de Gateway AntiVirus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados.

4.7 – PROTEÇÃO CONTRA-ATAQUES AVANÇADOS

4.7.1 – A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

4.7.2 – Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

4.7.3 – A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

4.7.4 – Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

4.7.5 – Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

4.7.6 – Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.

4.7.7 – Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

4.7.8 – Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.

4.7.9 – A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

4.7.10 – A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas.

4.7.11 – Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.

4.7.12 – Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

4.7.13 – Conter ameaças avançadas de dia zero.

4.7.14 – Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador.

4.7.15 – Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos.

4.7.16 – Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

4.7.17 – Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.

4.7.18 – Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.

4.7.19 – Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP , IMAP e CIFS.

4.7.20 – Mitigar ameaças de dia zero de forma transparente para o usuário final.

4.7.21 – Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.

4.7.22 – Implementar mecanismo de pesquisa por diferentes intervalos de tempo.

4.7.23 – Mitigar ameaças de dia zero via tráfego de internet.

4.7.24 – Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança.

4.7.25 – Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado.

4.7.26 – A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.

4.7.27 – Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.

4.7.28 – Conter e mitigar exploits avançados.

4.7.29 – A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-Vírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede).

4.7.30 – Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

4.7.31 – As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real.

4.7.32 – A Solução de segurança de FireWalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or buffering.

4.7.33 – A Solução deve unificar diversas funções de segurança em um único conjunto integrado, inspecionando os arquivos de usuários locais, remotos e móveis.

4.7.34 – A Solução deve unificar diversas funções de segurança em um único conjunto integrado inspecionando os arquivos de usuários locais, remotos e móveis.

4.7.35 – A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS etc., sem afetar o desempenho.

4.7.36 – A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças , com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

4.7.36.1 – Inspeção profunda de memória em tempo real;

4.7.36.2 – Inspeção profunda de pacotes livre de remontagem;

4.7.36.3 – Descriptografia e inspeção TLS/SSL;

4.7.36.4 – Inteligência e controle de aplicativos;

4.7.36.5 – Recursos SD-WAN seguros.

4.7.37 – É imprescindível que a solução não possua um limite de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

4.8 – CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB

4.8.1 – Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 50 (cinquenta) categorias distintas, com mecanismo de atualização e consulta automáticas.

4.8.2 – 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

4.8.3 – Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, 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.

4.8.4 – Permitir a customização de página de bloqueio.

4.8.5 – Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.

4.8.6 – Deve permitir submissão de novos sites para categorização.

4.8.7 – Permitir a classificação dinâmica de sitesweb, URLs e domínios.

4.8.8 – 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.

4.8.9 – Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.

4.8.10 – Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

4.9 – CARACTERÍSTICAS DE AUTENTICAÇÃO

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

4.9.2 – Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.

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

4.9.4 – Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.

4.9.5 – Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

4.9.6 – 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.

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

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

4.9.9 – Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

4.9.10 – A solução deve possibilitar SSO via API.

4.10 – CARACTERÍSTICAS DE ADMINISTRAÇÃO

4.10.1 – 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.

4.10.2 – Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.

4.10.3 – Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.

4.10.4 – Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração.

4.10.5 – Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.

4.10.6 – A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.

4.10.7 – 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.

4.10.8 – 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.

4.10.9 – Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.

4.10.10 – Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de “ICMP Unreachable” para máquina de origem

do tráfego, “TCP-Reset” para o cliente, “TCP-Reset” para o servidor ou para os dois lados da conexão.

4.10.11 – Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

4.10.12 – Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.

4.10.13 – Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.

4.10.14 – Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilzida por política, por protocolo TCP/UDP IPV4 e IPV6.

4.10.15 – Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.

4.10.16 – Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).

4.10.17 – Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.

4.10.18 – Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.

4.10.19 – A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.

4.10.20 – O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.

4.10.21 – O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.

4.10.22 – O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.

4.10.23 – O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.

4.10.24 – O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.

4.10.25 – O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

4.10.26 – A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto provisionamento da plataforma através de ponto central de gerenciamento.

4.10.27 –Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações

4.10.28 – A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas.

4.10.29 – Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful.

4.11 – GARANTIA

4.11.1 – A garantia dos equipamentos, software, suporte técnico, instalação e configuração após seu pleno funcionamento será de 90 (noventa) dias e de responsabilidade da empresa contratada, iniciando-se um dia útil após a emissão do Termo de Recebimento Definitivo.

4.11.2 – Durante o período indicado acima, qualquer atividade relacionada ao funcionamento dos produtos, como manutenção evolutiva, preventiva e corretiva, estará incluída na garantia, sem nenhum ônus para o Sescoop / MG. Após este período, a garantia deverá ser realizada pelo fabricante do equipamento.

4.11.3 – A garantia durante o período de 90 (noventa) dias deverá ser prestada pelo profissional indicado pela empresa contratada, conforme exigido no item 7.1, inciso III, alínea “b” e subitens.

5. FISCALIZAÇÃO E GESTÃO DO CONTRATO:

5.1 – Ao Sescoop / MG, por intermédio de sua Gerência de Tecnologia da Informação (GETIN), ficará assegurado o direito de fiscalizar o fornecimento / execução dos serviços pela empresa contratada, assim como questionar quaisquer eventualidades que desvirtuem o seu caráter intrínseco.

5.2 – O fornecimento / serviços prestados pela empresa contratada serão geridos pelo Sescoop / MG, através da Gerência de Licitações e Compras (GELIC).

ANEXO II

MODELO DE CARTA PROPOSTA

AO SERVIÇO NACIONAL DE APRENDIZAGEM DO COOPERATIVISMO DE MINAS GERAIS – SESCOOP / MG
COMISSÃO PERMANENTE DE LICITAÇÃO
PROCESSO LICITATÓRIO PREGÃO ELETRÔNICO 010/2024 (315855)

Prezados Senhores,

A empresa (Razão Social), inscrita no CNPJ sob o . . / - , com sede na (Endereço), neste ato representada pelo Sr. (a) , sócio proprietário / administrador / representante legal, Carteira de Identidade n.º , CPF n.º . . - , declara estar apresentando proposta comercial para a licitação em referência, cujo objeto é a **Contratação de empresa especializada para fornecimento de software, hardware, serviço de instalação, migração, configuração e otimização para solução de firewall, modelo SonicWall Gen 7 NSa 2700, com alta disponibilidade (HA – High Availability), contendo Advanced Protection Security Suite, pelo período de 36 (trinta e seis) meses, incluindo o suporte técnico do fabricante por igual período, para atender as necessidades do Sescoop / MG.**, comprometendo-se a assumir integralmente o fornecimento e prestação dos serviços pelos seguintes preços:

ITEM	QTDE.	DESCRIÇÃO. (A LICITANTE DEVERÁ DESCREVER, DETALHADAMENTE, OS EQUIPAMENTOS E SERVIÇOS QUE ESTÃO SENDO OFERTADOS, OBSERVANDO AS ESPECIFICAÇÕES DEFINIDAS NO ANEXO I).	VALOR UNITÁRIO	VALOR TOTAL
1	1	SonicWall Gen 7 NSa 2700 appliances 01 (ou superior do mesmo fabricante).	-	R$ ( )
2	1	SonicWall Gen 7 NSa 2700 appliances 02 (HA – High Availability).	-	R$ ( )
3	1	Software Advanced Protection Security Suite.	-	R$ ( )
4	1	Garantia do fornecedor (3 anos).	-	R$ ( )
5	1	Suporte técnico do fornecedor (3 anos).	-	R$ ( )
6	1	Serviço de instalação/migração, configuração e otimização.	-	R$ ( )
7	4	Fornecimento de 04 Cabos de Conexão Direta DAC SFP 10G 1,0 Metro.	R$ ( )	R$ ( )
VALOR GLOBAL DA PROPOSTA				**R$ ( )**

1) Declaramos, sob as penalidades da Lei, para fins de participação na licitação em referência, que a empresa:

a) Recebeu e estudou todos os documentos inerentes ao presente certame e tendo tomado conhecimento integral do teor do edital e seus anexos, sujeita-se às disposições nele contidas, em especial quanto ao anexo I (Termo de Referência);

b) Não foi declarada inidônea para licitar ou contratar com o SESCOOP, bem como comunicará qualquer fato ou evento superveniente quanto à habilitação ao certame supra, especificamente à capacidade jurídica e qualificação de regularidade fiscal;

c) Não possui em sua composição societária, como sócio ou administrador, dirigente ou empregado do SESCOOP.

2) Declaramos ainda que:

a) Nos valores acima discriminados estão incluídos todos os impostos, tributos, taxas, fretes, entrega (embarque e desembarque), prestação dos serviços, mão de obra, garantia, despesas com transporte e alimentação dos profissionais (se for o caso), encargos fiscais e comerciais e quaisquer outros encargos necessários ao cumprimento total da obrigação, ficando certo e esclarecido que o Sescoop / MG não se responsabilizará por quaisquer ônus ou despesas adicionais.

b) Concordamos com todas as cláusulas e condições estabelecidas no edital e em seus anexos e informamos que, caso sejamos vencedores do certame, assinaremos o Contrato de Fornecimento, realizando a entrega dos equipamentos e softwares no prazo máximo de 45 (quarenta e cinco) dias úteis, e executando os serviços, inclusive documentação, no prazo máximo de 30 (trinta) dias úteis após entrega dos equipamentos / softwares.

3) Informamos que o pagamento deverá ser realizado por meio de:

(☐) BOLETO (☐) CRÉDITO EM CONTA **(SELECIONAR A OPÇÃO DESEJADA)**

4) A validade da proposta é de 60 (sessenta) dias, contados da data agendada para realização da sessão.

5) O faturamento ocorrerá 100% (cem por cento) após a realização da entrega dos equipamentos e execução dos serviços e o pagamento será efetuado no prazo máximo de 28 (vinte oito) dias corridos.

Razão Social:
CNPJ:
Inscrição Estadual: (se houver)
Inscrição Municipal: (se houver)
Endereço completo:
Telefone: . Celular de Contato:
E-mail geral de contato da empresa licitante:
Dados Bancários:
Banco: n.º . Nome ( )
Agência: -
Conta corrente:

*Responsável(is) Legal(is) da empresa (conforme Contrato Social):
Nome:
Cargo:

Por ser verdade, firmamos a presente carta proposta.

, de de (local e data).

NOME LEGÍVEL E ASSINATURA DO RESPONSÁVEL LEGAL PELA EMPRESA LICITANTE

ANEXO III

MODELO DE ATESTADO DE CAPACIDADE TÉCNICA

Atestamos, a pedido da interessada e para fins de prova, que a empresa [**nome da empresa contratada, em negrito**], inscrita no CNPJ sob o nº 00.000.000/0001-00, estabelecida na Rua ....., nº....., bairro ....., na cidade de ....., Estado de ....., forneceu os equipamentos ..... e prestou os serviços correspondentes à ....., satisfatoriamente à [**nome da empresa contratante, em negrito**], CNPJ nº 00.000.000/0001-00, dentro dos prazos contratados.

Registramos, ainda, que a empresa cumpriu fielmente com suas obrigações, nada constando que a desabone técnica e comercialmente, até a presente data.

, de de (local e data).

_____

NOME LEGÍVEL, CPF E ASSINATURA DO RESPONSÁVEL LEGAL PELA EMPRESA EMITENTE DO ATESTADO

[endereço da empresa, carimbo, caso não possua papel timbrado]

ANEXO IV

MODELO DE DECLARAÇÃO DE PLENO ATENDIMENTO À HABILITAÇÃO

(Papel timbrado da Empresa)

AO SERVIÇO NACIONAL DE APRENDIZAGEM DO COOPERATIVISMO DE MINAS GERAIS – SESCOOP / MG
COMISSÃO PERMANENTE DE LICITAÇÃO

REF.: PREGÃO ELETRÔNICO 010/2024 (315855) – Contratação de empresa especializada para fornecimento de software, hardware, serviço de instalação, migração, configuração e otimização para solução de firewall, modelo SonicWall Gen 7 NSa 2700, com alta disponibilidade (HA – High Availability), contendo Advanced Protection Security Suite, pelo período de 36 (trinta e seis) meses, incluindo o suporte técnico do fabricante por igual período, para atender as necessidades do Sescoop / MG.

Prezados Senhores,

Empresa ....., inscrita no CNPJ n°....., por intermédio de seu representante legal o(a) Sr.(a)....., portador(a) da Carteira de Identidade nº..... e do CPF nº ....., vem pelo elo presente, declarar que cumpre plenamente aos requisitos da Proposta e dos documentos de Habilitação, exigidos no edital de licitação em referência.

, de de (local e data).

NOME LEGÍVEL E ASSINATURA DO RESPONSÁVEL LEGAL PELA EMPRESA LICITANTE

ANEXO V

DECLARAÇÕES – EXIGÊNCIAS LEGAIS

AO SERVIÇO NACIONAL DE APRENDIZAGEM DO COOPERATIVISMO DE MINAS GERAIS – SESCOOP / MG
COMISSÃO PERMANENTE DE LICITAÇÃO

REF.: PREGÃO ELETRÔNICO 010/2024 (315855) – Contratação de empresa especializada para fornecimento de software, hardware, serviço de instalação, migração, configuração e otimização para solução de firewall, modelo SonicWall Gen 7 NSa 2700, com alta disponibilidade (HA – High Availability), contendo Advanced Protection Security Suite, pelo período de 36 (trinta e seis) meses, incluindo o suporte técnico do fabricante por igual período, para atender as necessidades do Sescoop / MG.

Empresa ....., inscrita no CNPJ n°....., por intermédio de seu representante legal o(a) Sr.(a)....., portador(a) da Carteira de Identidade nº ..... e do CPF nº ....., **DECLARA sob as penas da Lei:**

a) Que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos;

b) Que, até a presente data inexiste(m) fato(s) impeditivo(s) para a sua habilitação, estando ciente da obrigatoriedade de declarar ocorrências posteriores;

c) Ter recebido todos os documentos e informações, conhecer e acatar as condições para o cumprimento das obrigações objeto da licitação;

d) Que inexistem impedimentos para sua participação na licitação, não incorrendo em nenhum dos casos relacionados no item 3 do edital;

e) Que a proposta apresentada foi elaborada de maneira independente, que não tentou influir na decisão de qualquer outro potencial participante desta licitação, e que com estes ou com outras pessoas não discutiu nem recebeu informações.

, de de (local e data).

NOME LEGÍVEL E ASSINATURA DO RESPONSÁVEL LEGAL PELA EMPRESA LICITANTE

ANEXO VI

MODELO DE DECLARAÇÕES – EXIGÊNCIAS LEGAIS DE PROTEÇÃO DE DADOS

AO SERVIÇO NACIONAL DE APRENDIZAGEM DO COOPERATIVISMO DE MINAS GERAIS – SESCOOP / MG
COMISSÃO PERMANENTE DE LICITAÇÃO

REF.: PREGÃO ELETRÔNICO 010/2024 (315855) – Contratação de empresa especializada para fornecimento de software, hardware, serviço de instalação, migração, configuração e otimização para solução de firewall, modelo SonicWall Gen 7 NSa 2700, com alta disponibilidade (HA – High Availability), contendo Advanced Protection Security Suite, pelo período de 36 (trinta e seis) meses, incluindo o suporte técnico do fabricante por igual período, para atender as necessidades do Sescoop / MG.

Empresa ....., inscrita no CNPJ n°....., por intermédio de seu representante legal o(a) Sr.(a)....., portador(a) da Carteira de Identidade no..... e do CPF no ....., DECLARA sob as penas da Lei:

I – Que está ciente dos direitos, obrigações e penalidades aplicáveis constantes da Lei Geral de Proteção de Dados Pessoais – "LGPD" (Lei 13.709/2018), e obrigam-se a adotar todas as medidas razoáveis par garantir, por si, bem como seu pessoal, colaboradores, empregados e subcontratados que utilizem os Dados Protegidos na extensão autorizada na referida LGPD.

II – Que mantém sigilo das informações e dos dados que trata, sejam pessoais ou não, além de se manter alinhado com as boas práticas de segurança e trato tecnológico, e com as práticas mais avançadas de governança.

III – Não compartilha com terceiros, parceiros ou em qualquer negociação comercial, as informações coletadas. Toda e qualquer informação a respeito dos clientes e usuários do Sescoop / MG somente serão repassadas mediante aprovação expressa destes ou por ordem judicial.

IV – Atua em consonância com sua missão institucional, respeitando o direito à privacidade e visando o melhor uso da tecnologia da informação para a garantia da segurança dos dados de seus associados, fornecedores e parceiros.

V – Estar em conformidade com a legislação vigente e adequada à Lei nº 13.709, de 14 de agosto de 2018, e demais regulações quanto ao tema. Declara, ainda, que os princípios norteadores da referida legislação estão incorporados no desenvolvimento de suas atividades institucionais, bem como na prática de seus agentes de tratamento.

, de de (local e data).

NOME LEGÍVEL E ASSINATURA DO RESPONSÁVEL LEGAL PELA EMPRESA LICITANTE

TIPO: CPS
Nº: 0XX/2024

ANEXO VII

MINUTA DE CONTRATO

CONTRATO que entre si celebram o Serviço Nacional de Aprendizagem do Cooperativismo de Minas Gerais – SESCOOP/MG e a XXXXXXXXXXXXXX.

CLÁUSULA PRIMEIRA: DAS PARTES

1.1. **SERVIÇO NACIONAL DE APRENDIZAGEM DO COOPERATIVISMO DE MINAS GERAIS – SESCOOP/MG**, doravante denominado CONTRATANTE, situado na Rua Ceará, nº 771, Bairro Santa Efigênia, Cidade Belo Horizonte/MG – CEP 30.150-312, inscrita no CNPJ nº 07.064.534/0001-20 e Inscrição Estadual Isento, neste ato representado pelo seu superintendente ALEXANDRE GATTI LAGES, portador do CPF nº 005.XXX.3XX-22 e por sua gerente geral ISABELA CHENNA PEREZ, portadora do CPF nº 074.XXX.7XX-85.

1.2. **XXXXXXXXXXXXXXXXXXXXXXXXXXXX,** doravante denominada **CONTRATADA,** situada na Rua XXXXXXXXXXX, nº XXXX, Bairro XXXXXXXXX, CEP XXXXXXXX, cidade XXXXXX, inscrita no CNPJ XXXXXXXXXXXXXX, representada neste ato por XXXXXXXXXXXXX, portador do CPF nº XXXXXXXXXXX.

CLÁUSULA SEGUNDA: DO OBJETO

2.1. Constitui objeto deste CONTRATO a prestação de serviços fornecimento de software, hardware, serviço de instalação, migração, configuração e otimização para solução de firewall, modelo SonicWall Gen 7 NSa 2700, com alta disponibilidade (HA – High Availability), contendo Advanced Protection Security Suite, pelo período de 36 (trinta e seis) meses, incluindo o suporte técnico do fabricante por igual período, para atender as necessidades do CONTRATANTE.

CLÁUSULA TERCEIRA: ESCOPO DA EXECUÇÃO DOS SERVIÇOS

3.1. Os equipamentos e softwares deverão ser entregues no prazo máximo de 45 (quarenta e cinco) dias úteis, e os serviços realizados, inclusive documentação, no prazo máximo de 30 (trinta) dias úteis após entrega dos equipamentos / softwares, diretamente na Sede do CONTRATANTE, localizada na Rua Ceará, nº 771, Bairro Santa Efigênia, CEP 30150-311, em Belo Horizonte/MG.

3.1.1. O prazo se inicia a partir da data de vigência prevista na cláusula XXX, deste contrato.

3.2. Previamente à entrega/execução dos serviços, a CONTRATADA deverá obrigatoriamente, efetuar contato com a Gerência de Tecnologia da Informação (GETIN) do CONTRATANTE, cujos dados para contato são: getin@sistemaocemg.coop.br e moacir.junior@sistemaocemg.coop.br, visando pactuar as especificidades da entrega/execução dos serviços e demais informações que se fizerem necessárias.
3.3. Por ocasião da entrega dos equipamentos/softwares e realização dos serviços, a contratada deverá observar rigorosamente as especificações técnicas descritas na cláusula décima. A não obediência a este quesito acarretará a devolução sumária dos equipamentos/serviços e a aplicação das penalidades cabíveis.
3.4. Os equipamentos entregues deverão ser novos, de 1º uso e em linha de produção mais recente, igual ou superior tecnologicamente, à época de aquisição, não sendo aceito equipamentos utilizados em exposições, feiras ou eventos promocionais.
3.5. Os equipamentos entregues em desconformidade com as especificações especificadas neste contrato serão passíveis de devolução à contratada, cabendo a esta todo e quaisquer ônus decorrentes, inclusive, se for o caso, o cancelamento de Nota Fiscal, mesmo que emitida em mês anterior, ficando entendido que

a entrega de equipamentos em desconformidade é considerada falta grave, podendo ensejar a aplicação das penalidades cabíveis.
3.6. Os equipamentos entregues estão sujeitos à inspeção pelo CONTRATANTE, que poderá rejeitá-los (no todo ou em parte) se considerá-los defeituosos ou divergentes com relação às especificações. Os equipamentos rejeitados serão restituídos à CONTRATADA, por sua conta e risco. Todas as despesas com desembalagem, reembalagem e devolução dos equipamentos serão debitadas à contratada.
3.7. A realização dos serviços deverá ser efetuada por técnicos da contratada/fabricante, sendo acompanhada por técnicos indicados pelo CONTRATANTE.
3.8. O atraso na entrega dos equipamentos/softwares e execução dos serviços ensejará a aplicação da multa, conforme previsto neste contrato.
3.9. Eventuais solicitações de prorrogação do prazo de entrega somente serão analisadas se atenderem às seguintes condições:

a) O pedido for encaminhado à Comissão Permanente de Licitação, sendo desconsiderados para efeito de isenção de multa, os pedidos encaminhados diretamente à outras Gerências do contratante, mesmo que deferidos;
b) O pedido for enviado à Comissão Permanente de Licitação antes de expirada a data de entrega contratada. Vencida a data de entrega não haverá isenção de multas;
c) O eventual atraso decorrer de caso fortuito ou força maior, assim entendidas as circunstâncias absolutamente imprevisíveis e insuperáveis por parte da contratada. A falta de programação, ou acordo, ou entendimento entre a contratada e seus fornecedores/fabricantes não são motivos para prorrogação da data.

3.10. O pedido de prorrogação será analisado pela Comissão Permanente de Licitação, podendo ser deferido ou indeferido, formalmente, ficando certo e esclarecido que o indeferimento não desobriga a contratada de entregar os equipamentos, sujeitando-se a mesma, neste caso, às penalidades cabíveis. A negativa de entrega, em face do indeferimento, será considerada falta grave, podendo ensejar a suspensão do direito de licitar e contratar com o SESCOOP, nos termos de seu regulamento.
3.11. A aceitação dos equipamentos/serviços não exime a CONTRATADA da responsabilidade quanto à qualidade dos mesmos e não invalida qualquer reclamação posterior do CONTRATANTE.
3.12. A CONTRATADA deverá executar todo o serviço necessário a plena operacionalização da solução ofertada, devendo obrigatoriamente incluir todos os serviços abaixo:

a) Reunião de Quick off do projeto;
b) Planejamento detalhado dos procedimentos a serem executados;
c) Apresentação ao cliente do cronograma e processos para aprovação;
d) Instalação física dos componentes de hardware fornecidos no rack do CONTRATANTE;
e) Interligação dos componentes de hardware fornecidos a rede/links do CONTRATANTE de forma redundante;
f) Prestar auxílio em qualquer configuração de rede necessária a instalação da solução;
g) Instalação do licenciamento necessário;
h) Atualização de firmware dos componentes de hardware fornecidos;
i) Configuração da alta disponibilidade do hardware fornecido;
j) Levantamento de todas as regras de firewall, filtros de conteúdo, IPS, IDS, anti-malware e demais proteções existentes nos firewalls antigos do CONTRATANTE;
k) Migração, ajustes e otimização de todas as regras de firewall e demais configurações de controle e segurança aos novos firewalls;
l) Criar ou ajustar novas políticas de segurança conforme definição do CONTRATANTE;
m) Criar ou ajustar novas regras de firewall conforme definição do CONTRATANTE;
n) Implementar, criar ou ajustar um ambiente seguro de Captive Portal corporativo seguindo as melhores práticas;
o) Configurar e atualizar os relatórios existentes no software Global Management System (GMS) atualmente instalado e licenciado no CONTRATANTE;
p) Proceder a testes de funcionalidade antes da entrada em produção;

q) Proceder o acompanhamento da entrada em produção de forma presencial ou remota, dependendo da criticidade no ambiente do CONTRATANTE, com no mínimo 7 dias de acompanhamento;
r) Proceder aos ajustes necessários para solução dos problemas apresentados durante a entrada em produção;
s) Proceder a documentação completa contendo o passo a passo da nova solução instalada;
t) Proceder a um treinamento hands-on de no mínimo 8 horas sobre a solução instalada, incluindo o gerenciamento básico dos recursos migrados/ativos da solução de firewall, relatórios;
u) A CONTRATADA deverá obrigatoriamente registar os novos equipamentos na conta institucional do CONTRATANTE no site MySonicWall (https://www.mysonicwall.com/).

3.13. Quaisquer outros serviços necessários ao pleno funcionamento da solução deverão ser executados pela contratada mesmo que não estejam listados acima.
3.14. Todos os serviços devem ser executados de forma a não gerar paradas no ambiente de produção do CONTRATANTE durante o horário comercial. Serviços com risco ou necessidade de parada do ambiente de produção, deverão obrigatoriamente ser executados fora de horário comercial.
3.15. A contratada deve estar ciente que o CONTRATANTE não executará serviços que só podem ser realizados presencialmente. De forma explicita ficam definidos que os serviços de instalação física, serão obrigatoriamente executados de forma presencial no endereço do CONTRATANTE e não permitem negociação de atendimento remoto pela contratada.
3.16. A contratada deverá fornecer 04 (quatro) cabos de conexão direta DAC SFP 10G 1,0 metro.

CLÁUSULA QUARTA: DO PREÇO E FORMA DE PAGAMENTO

4.1. Para a realização do objeto deste **CONTRATO**, o **CONTRATANTE** repassará à **CONTRATADA**, o valor total de **R$XXX.XXX,00 (XXXXXXXXXXXX mil reais),** conforme valores unitários especificados abaixo:

XXXX

4.2. O faturamento ocorrerá 100% (cem por cento) após a realização da entrega dos equipamentos/softwares, bem como realização dos serviços. Sendo o pagamento efetuado no prazo máximo de 28 (vinte oito) dias corridos, mediante a apresentação da Nota Fiscal/Fatura pela CONTRATADA, devidamente aprovada pela Gerência de Licitações e Compras do CONTRATANTE, sem prejuízo de eventuais multas por atraso.
4.3. A nota fiscal / fatura deverá ser encaminhada para o e-mail notasfiscais@sistemaocemg.coop.br contendo os dados bancários para pagamento, que será realizado preferencialmente via depósito em conta.
4.4. No caso de emissão de Nota Fiscal na forma “eletrônica”, a contratada fica obrigada a enviar juntamente com o documento o arquivo eletrônico denominado “XML” para fins de conferência e fechamento junto a receita estadual. A Nota Fiscal ficará retida para pagamento, até o envio do presente arquivo.
4.5. Não será aceita Nota Fiscal / Fatura de serviços emitida entre o dia 21 e 31 de determinado mês. A ocorrência de tal fato implicará na devolução sumária, ficando a contratada obrigada a substituir o documento.
4.6. O CONTRATANTE poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela empresa contratada, nos termos deste contrato.
4.7. No caso de incorreção na Nota Fiscal, esta será restituída à contratada para as correções solicitadas. O prazo de pagamento será contado a partir da data da regularização do documento fiscal, não respondendo o contratante por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.
4.8. Caso os equipamentos e serviços constantes da Nota Fiscal/Fatura estejam em desacordo com os equipamentos entregues/serviços executados, ela não será liberada para pagamento, até a correção do

fato. Caberá à contratada a solução do problema para aprovação dos equipamentos/serviços pelo CONTRATANTE e liberação do pagamento.
4.9. O CONTRATANTE fará a retenção dos impostos de acordo com a legislação vigente, caso aplicável.

4.9.1. Retenção de Imposto Sobre Serviço de Qualquer Natureza (ISSQN): de acordo com a Legislação, as Microempresas ou as Empresas de Pequeno Porte, optantes pelo Simples Nacional, que não informarem, a alíquota de retenção nos documentos fiscais, será aplicada a alíquota de 5% (cinco por cento).

4.10. A Nota Fiscal/Fatura deverá ser emitida pela contratada, obrigatoriamente com o número de inscrição do CNPJ apresentado no processo de contratação, não se admitindo Nota Fiscal/Fatura emitida com outro CNPJ, mesmo de filiais ou da matriz da CONTRATADA.
4.11. Salvo autorização expressa e por escrito do CONTRATANTE, é vedado à CONTRATADA, seja por qual motivo for, o desconto ou negociação de duplicatas, faturas e afins em instituições financeiras, relativamente a parcelas de pagamento vinculadas ao fornecimento / execução dos serviços do objeto deste contrato.

CLÁUSULA QUINTA: DA RESCISÃO

5.1. Qualquer dos partícipes poderá denunciar o presente CONTRATO por meio de comunicação escrita, com antecedência mínima de 10 (dez) dias. Ficando as partes responsáveis pelas obrigações decorrentes do tempo de vigência e creditando-lhes, igualmente, os benefícios adquiridos no mesmo período.
5.2. Constitui motivo para rescisão deste CONTRATO, independentemente do instrumento de sua formalização, o inadimplemento de qualquer item pactuado, particularmente quando constatadas as seguintes situações:

5.2.1. Não cumprimento de cláusulas ou prazos constantes neste CONTRATO;
5.2.2. Cumprimento irregular das cláusulas ou prazos constantes deste CONTRATO;
5.2.3. Paralisação da execução do objeto deste CONTRATO, sem a justa causa e prévia comunicação ao CONTRATANTE;
5.2.4. A associação da CONTRATADA com outrem, ainda a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não são admitidas neste CONTRATO;
5.2.5. Desatendimento das determinações regulares da autoridade designada para acompanhar a execução deste CONTRATO, assim como a de seus superiores;
5.2.6. Cometimento reiterado das faltas na execução deste CONTRATO;
5.2.7. Alteração social ou modificação da finalidade ou da estrutura da instituição que, a juízo do CONTRATANTE, prejudique a execução do objeto deste CONTRATO;
5.2.8. A ocorrência de caso fortuito ou de força maior, regularmente comprovado, impeditiva da execução deste CONTRATO;
5.2.9. Prática de atos ilícitos visando frustrar os objetivos deste CONTRATO;
5.2.10. Cometimento de falhas ou fraudes na execução do objeto deste CONTRATO;
5.2.11. Inadimplência total do objeto deste CONTRATO.

5.3. Os casos de rescisão serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa, no prazo de 10 (dez) dias, a contar do recebimento da notificação extrajudicial.
5.4. Se o presente CONTRATO for rescindido, o Termo de Rescisão deverá discriminar:

5.4.1. Balanço dos eventos já cumpridos ou parcialmente cumpridos; e
5.4.2. Relação dos pagamentos já efetuados ou ainda devidos.

CLÁUSULA SÉXTA: DO ACOMPANHAMENTO

6.1. Ao CONTRATANTE fica assegurado o direito de exercer controle e fiscalização sobre a execução dos trabalhos desenvolvidos pela CONTRATADA, através da Gerência da Tecnologia da Informação (GETIN),

através do empregado MOACIR LOURENÇO ROSA JUNIOR, ou na falta deste, por quem o CONTRATANTE indicar para cumprir a função, assim como questionar quaisquer eventualidades que desvirtuem o caráter intrínseco do mesmo.
6.2. Caberá à CONTRATADA apresentar responsável pelo acompanhamento do projeto apresentado.
6.3. Caso a contratada, no decorrer da prestação dos serviços, demonstre inaptidão técnica, operacional ou administrativa, bem como quaisquer outras características que, no entendimento do CONTRATANTE, possa prejudicar, inviabilizar, retardar ou desvirtuar o objetivo pretendido, poderá a entidade aplicar as penalidades previstas no presente Contrato.
6.4. A gestão corporativa do contrato será realizada pela Gerência de Licitações e Compras (GELIC).

CLÁUSULA SÉTIMA: DA VIGÊNCIA

7.1. A vigência do presente **CONTRATO** iniciar-se-á na data de XX de julho de 2024 e findar-se-á em XX de XXXXX de 2024, podendo ser prorrogado, mediante acordo prévio entre as **PARTES**, retratado através de Termo Aditivo.

CLÁUSULA OITAVA: DOS ENCARGOS

8.1. Será de exclusiva responsabilidade da CONTRATADA o pagamento dos encargos trabalhistas, previdenciários e aqueles relacionados à prevenção de acidentes de trabalho, de seus funcionários, não decorrendo do presente CONTRATO, qualquer vínculo empregatício com o CONTRATANTE ou eventuais prepostos.

8.1.1. Fica expressamente convencionado que, na hipótese de uma das partes ser autuada, notificada, intimada ou condenada, por qualquer obrigação comprovadamente de responsabilidade da outra parte, seja de que natureza for, mesmo após o término do CONTRATO, a parte inocente deverá notificar a parte infratora para que esta, no prazo de até 30 (trinta) dias, contados do recebimento de tal notificação, cumpra a obrigação determinada;
8.1.2. Caberá à CONTRATADA, informar aos seus parceiros e empregados envolvidos na execução das ações educativas, o conteúdo do presente CONTRATO.

8.2. A CONTRATADA deverá efetuar, por sua conta, o pagamento dos impostos, licenças e taxas federais, estaduais e municipais, incidentes sobre sua atividade ou decorrentes desta parceria, comprovando tais pagamentos ao CONTRATANTE ou, reconhecimento de isenções e imunidades, sempre que este solicitar, formalmente.

CLÁUSULA NONA: PENALIDADES

9.1. A inexecução total ou parcial injustificada, a execução deficiente, irregular ou inadequada do objeto do presente contrato, assim como o descumprimento dos prazos e condições estipulados e, sem prejuízo, implicarão nas penalidades abaixo mencionadas:

9.1.1. Advertência;
9.1.2. Cancelamento do contrato;
9.1.3. Multa por não realização dos serviços;
9.1.4. Suspensão do direito de licitar ou contratar com o Sescoop, por prazo não superior a 5 (cinco) anos.
9.1.5. Será cobrada multa por atraso na entrega dos equipamentos e softwares e na execução dos serviços, no percentual de 0,5% (meio por cento) ao dia, referente a parcela em atraso, limitada a 10% (dez por cento) do valor total do CONTRATO.

9.2. Ocorrendo a aplicação de multa, esta será descontada sobre o valor da nota fiscal/fatura ou dos créditos a que a empresa CONTRATADA fizer “jus”, no ato do pagamento, ou recolhidas diretamente à tesouraria do CONTRATANTE, ou ainda, quando for o caso, cobrada judicialmente;

9.3. Para aplicação das penalidades aqui previstas, a CONTRATADA será notificada para apresentação de defesa prévia, no prazo de 05 (cinco) dias, contados da notificação.
9.4. As penalidades previstas são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, sem prejuízo de outras medidas cabíveis, tal como a rescisão contratual.

CLÁUSULA DÉCIMA: ESPECIFICAÇÃO TÉCNICA DA FERRAMENTA FIREWALL

10.1. Compete a CONTRATADA fornecer os seguintes itens para execução do objeto:

PRODUTO SOLUÇÃO DE FIREWALL	QUANTIDADE
SonicWall Gen 7 NSa 2700 appliances 01 (ou superior do mesmo fabricante).	01
SonicWall Gen 7 NSa 2700 appliances 02 (HA – High Availability).	
Software Advanced Protection Security Suite.	
Garantia do fornecedor (3 anos).	
Suporte técnico do fornecedor (3 anos).	
Serviço de instalação/migração, configuração e otimização.	
Fornecimento de 04 Cabos de Conexão Direta DAC SFP 10G 1,0 Metro.	04

10.2. Os equipamentos e serviços deverão preencher os seguintes requisitos mínimos:

10.2.1. O equipamento deve ser obrigatoriamente novo, em linha de montagem e de primeiro uso, podendo, a critério da empresa contratada, utilizar ou não o sistema de benefícios SonicWall Secure Upgrade appliance.
10.2.2. Fornecimento e instalação do software de segurança Advanced Protection Security Suite com todas suas features habilitadas durante 3 (três) anos em ambos os appliances fornecidos na solução com alta disponibilidade (HA).
10.2.3. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 3.0 Gbps ou superior.
10.2.4. Desempenho em modo de Inspeção (descriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 800 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.
10.2.5. Desempenho mínimo de 3.4 Gbps de IPS.
10.2.6. Suporte mínimo de 1.500.000 conexões simultâneas/concorrentes no modo SPI.
10.2.7. Suporte mínimo de 21.000 novas conexões por segundo.
10.2.8. Deve possuir armazenamento interno de no mínimo 64 GB e suportar expansão de armazenamento interno para até 256Gb.
10.2.9. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.
10.2.10. Deve possuir 16 interfaces 1 GbE padrão RJ-45.
10.2.11. Deve possuir 3 interfaces 10GbE SFP+.
10.2.12. Deve possuir 1interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.
10.2.13. Deve possuir 2 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.
10.2.14. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1000 usuários simultâneos.
10.2.15. A VPN SSL deve ser licenciada para, no mínimo, 02 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 500 usuários simultâneos.
10.2.16. Deve suportar 2000 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.
10.2.17. Deve suportar, no mínimo, 2.1Gbps de desempenho de VPN IPSEC.
10.2.18.O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.
10.2.19. O Equipamento deverá ser homologado pela ANATEL.

10.2.20. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.
10.2.21. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no mínimo 36 (trinta e seis) meses.
10.2.22. É imprescindível que a solução não possua um limite de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

10.3. Os FIREWALLS FÌSICOS deverão preencher as seguintes características e especificações:

10.3.1. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.
10.3.2. Para proteção do ambiente contra-ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.
10.3.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.
10.3.4. Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade.
10.3.5. 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.
10.3.6. Os firewalls devem ser entregues com licenciamento válido para, no mínimo, 36 meses, incluindo garantia e suporte.
10.3.7. Deverá ser fornecido suporte técnico com a fabricante do produto durante 36 meses no mínimo.

10.4. A CONTRATADA deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.
10.5. A CONTRATADA deve 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 (NAT-T) e NAT dentro do tunel IPSec.
10.6. A CONTRATADA deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
10.7. A CONTRATADA deve fornecer proteção anti-spoofing.
10.8. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;
10.9. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.
10.10. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação.
10.11. A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.
10.12. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

a) Latência;
b) Jitter;
c) Perda de pacotes.

10.13. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal logico.

10.14. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.
10.15. A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.
10.16. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
10.17. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.
10.18. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.
10.19. 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 via VPN.
10.20. Deve suportar DHCP relay.
10.21. 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 serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.
10.22. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (física e virtual) ou zona de segurança.
10.23. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.
10.24. Deve ter suporte à proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.
10.25. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.
10.26. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood etc.
10.27. Detectar e bloquear a origem de portscans.
10.28. Deve permitir o bloqueio de ataques.
10.29. Deve permitir o bloqueio de exploits conhecidos.
10.30. O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP e SMTP.
10.31. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser descriptografado de forma transparente à aplicação.
10.32. Implementar DSCP (Differentiated Services Code Points).
10.33. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, 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 da rede.
10.34. Implementar controle e gerenciamento de banda para a tecnologia VoIP(Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.
10.35. Implementar mecanismo de sincronismo de horário através do protocolo NTP.
10.36. Possuir suporte ao protocolo SNMP versões 2 e 3.
10.37. Possuir suporte a log via syslog.
10.38. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.
10.39. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada

mudança de versão, ou após determinado período, e baseado em normas nacionais e internacionais de segurança da informação.
10.39. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes.
10.40. 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 e-mail.
10.41. Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.
10.42. Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3.
10.43. Deve permitir a funcionalidade de ARP bridging.
10.44. Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm".
10.45. A CONTRATADA deverá fornecer o VPN com as seguintes características:

10.45.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.
10.45.2. Suportar algoritmos de criptografia 3DES, AES 128 e AES 256.
10.45.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.
10.45.4. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.
10.45.5. Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.
10.45.6. Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.
10.45.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.
10.45.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.
10.45.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.
10.45.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.
10.45.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.
10.45.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.
10.45.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.
10.45.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.
10.45.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.
10.45.16. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

10.46. DA ALTA DISPONIBILIDADE (HA)

10.46.1. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. 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.
10.46.2. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Passivo, com as implementações de Failover.
10.46.3. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.
10.46.4. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.
10.46.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.
10.46.6. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.
10.46.7. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.
10.46.8. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.
10.46.9. A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que haja perda das conexões de VPN, FTP, Oracle SQL*NET, RSTP, Real Audio, VPN Client, Dynamic Arp Objects, Informações de DHCP Server, Multicast , IGMP, Usuários ativos, RIP e OSPF.

10.47. DO CONTROLE DE AMEAÇAS

10.47.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.
10.47.2. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.
10.47.3. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.
10.47.4. Implementar funcionalidade de detecção e bloqueio de “call-backs”.
10.47.5. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.
10.47.6. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.
10.47.7. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.
10.47.8. Implementar interface CLI segura através do protocolo SSH.
10.47.9. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.
10.47.10. A solução deve permitir criar regras de exceção de acordo com a proteção.
10.47.11. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;
10.47.12. Permitir o bloqueio de malwares (vírus, worms, spyware etc.).
10.47.13. A solução deve ser capaz de proteger contra-ataques a DNS.
10.47.14. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.
10.47.15. A solução deve ser capaz de prevenir acesso a websites maliciosos.
10.47.16. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.
10.47.17. A solução deverá receber atualizações de um serviço baseado em cloud.

10.47.18. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.
10.47.19. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.
10.47.20. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade.
10.47.21. A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown.
10.47.22. A solução de Gateway AntiVirus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados.

10.48. PROTEÇÃO CONTRAATAQUES AVANÇADOS

10.48.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.
10.48.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.
10.48.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.
10.48.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.
10.48.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.
10.48.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.
10.48.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.
10.48.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.
10.48.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.
10.48.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas.
10.48.11. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.
10.48.12. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego.
10.48.13. Conter ameaças avançadas de dia zero.
10.48.14. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador.
10.48.15. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos.
10.48.16. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.
10.48.17. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.
10.48.18. Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.
10.48.19. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS.

10.48.20. Mitigar ameaças de dia zero de forma transparente para o usuário final.
10.48.21. Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.
10.48.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo.
10.48.23. Mitigar ameaças de dia zero via tráfego de internet.
10.48.24. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança.
10.48.25. Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado.
10.48.26. A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.
10.48.27. Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.
10.48.28. Conter e mitigar exploits avançados.
10.48.29. A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-Vírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede).
10.48.30. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.
10.48.31. As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real.
10.48.32. A Solução de segurança de FireWalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or buffering.
10.48.33 .A Solução deve unificar diversas funções de segurança em um único conjunto integrado, inspecionando os arquivos de usuários locais, remotos e móveis.
10.48.34. A Solução deve unificar diversas funções de segurança em um único conjunto integrado inspecionando os arquivos de usuários locais, remotos e móveis.
10.48.35. A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS etc., sem afetar o desempenho.
10.48.36. A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças , com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

a) Inspeção profunda de memória em tempo real;
b) Inspeção profunda de pacotes livre de remontagem;
c) Descriptografia e inspeção TLS/SSL;
d) Inteligência e controle de aplicativos;
e) Recursos SD-WAN seguros.

10.48.37. É imprescindível que a solução não possua um limite de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

10.49. CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB

10.49.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 50 (cinquenta) categorias distintas, com mecanismo de atualização e consulta automáticas.
10.49.2. 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.
10.49.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, 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.
10.49.4. Permitir a customização de página de bloqueio.
10.49.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.
10.49.6. Deve permitir submissão de novos sites para categorização.
10.49.7. Permitir a classificação dinâmica de sitesweb, URLs e domínios.
10.49.8. 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.
10.49.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.
10.49.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

10.50. CARACTERÍSTICAS DE AUTENTICAÇÃO

10.50.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.
10.50.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.
10.50.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.
10.50.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.
10.50.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.
10.50.6. 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.
10.50.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.
10.50.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.
10.50.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.
10.50.10. A solução deve possibilitar SSO via API.

10.51. CARACTERÍSTICAS DE ADMINISTRAÇÃO

10.51.1. 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.
10.51.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.
10.51.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.
10.51.4. Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração.
10.51.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.

10.51.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.
10.51.7. 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.
10.51.8. 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.
10.51.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.
10.51.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de “ICMP Unreachable” para máquina de origem do tráfego, “TCP-Reset” para o cliente, “TCP-Reset” para o servidor ou para os dois lados da conexão.
10.51.11. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.
10.51.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.
10.51.13 Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.
10.51.14. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilzida por política, por protocolo TCP/UDP IPV4 e IPV6.
10.51.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.
10.51.16. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).
10.51.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.
10.51.18. Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.
10.51.19. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.
10.51.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.
10.51.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.
10.51.22. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.
10.51.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.
10.51.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.
10.51.25. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.
10.51.26. A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto provisionamento da plataforma através de ponto central de gerenciamento.
10.51.27. Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise

de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações
10.51.28. A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas.
10.51.29. Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful.

CLÁUSULA DÉCIMA PRIMEIRA: DA CONFIDENCIALIDADE

11.1. As PARTES reconhecem que todas as informações, de qualquer natureza, eventualmente reveladas pelas partes, sejam feitas em meio físico, magnético ou oralmente, durante a vigência do presente contrato, incluídas, mas não se limitando à base de dados técnicos, planos comerciais ou estratégicos, informações financeiras e projeções, dados ou informações sobre o mercado, clientes, parceiros, fornecedores ou equipamentos, documentos, projetos, ou até mesmo correspondências classificadas como informações confidenciais e sobre as mesmas deverá ser guardado sigilo absoluto, para todos os efeitos.
11.2. A obrigação de confidencialidade de que trata o presente contrato visa proteger os direitos e interesses de todo gênero das partes, buscando impedir a revelação e a utilização indevida das Informações Confidenciais, motivo pelo qual as partes obrigam-se, de forma perene, em caráter irretratável e irrevogável, a manter sob sigilo absoluto todas as Informações Confidenciais a que vier a ter acesso, tratando-as como segredo industrial e de negócios.
11.3. É vedado à CONTRATADA divulgar informação, dado ou modelo que tenha sido desenvolvido a partir de qualquer Informação Confidencial, bem como desenvolver produtos, métodos ou serviços com base tanto nas Informações Confidenciais, como nas demais informações e conhecimentos obtidos no desenvolvimento do propósito deste contrato, sem qualquer exceção.
11.4. A CONTRATADA declara-se ciente e concorda, bem como adotará todas as medidas para deixar seus parceiros, Colaboradores e clientes também cientes, e que a executora em decorrência do presente contrato poderá ter acesso, utilizará, e processará, eletrônica e manualmente, informações e dados prestados pela executora e seus clientes (“Dados Protegidos”).
11.5. As Partes declaram-se cientes dos direitos, obrigações e penalidades aplicáveis constantes da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) (“LGPD”), e obrigam-se a adotar todas as medidas razoáveis par garantir, por si, bem como seu pessoal, colaboradores, empregados e subcontratados que utilizem os Dados Protegidos na extensão autorizada na referida LGPD.
11.6. As Partes declaram-se cientes dos direitos, obrigações e penalidades aplicáveis constantes da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) (“LGPD”), e se comprometem a realizar o tratamento de Dados Pessoais aos quais obtenham acesso em decorrência deste Contrato de acordo com a legislação aplicável, incluindo, mas não se limitando à Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), Lei 12.965/2014 (Marco Civil da Internet), Decreto n. 8.771/2016 (Regulamento do Marco Civil da Internet), bem como quaisquer outras leis ou normas relativas à proteção de dados pessoais que vierem a ser promulgadas ou entrarem em vigor no curso da vigência deste contrato. E obrigam-se a adotar todas as medidas razoáveis par garantir, por si, bem como seu pessoal, colaboradores, empregados e subcontratados que utilizem os Dados Protegidos na extensão autorizada na referida LGPD.
11.7. O CONTRATANTE está comprometido em assegurar que o controle sobre os dados pessoais. Para isso, atua fortemente para garantir que sua privacidade e a proteção dos seus dados pessoais sejam observadas quando você está nos nossos ambientes físicos ou quando acessa nossos ambientes digitais. Coletamos e tratamos os dados pessoais, de acordo com nosso Aviso de Privacidade disponível em: https://sistemaocemg.coop.br/evento/portal-da-privacidade/?categories=10%3B e em conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD, o Marco Civil da Internet e outras Leis ou regulamentos aplicados ao tema.
11.8. A CONTRATADA declara estar ciente que quaisquer comunicações e/ou solicitações relacionadas à proteção de dados pessoais decorrentes do presente instrumento deverão ser realizadas exclusivamente através do canal oficial estabelecido pelo SESCOOP/MG: dpo@sistemaocemg.coop.br.
11.9. A CONTRATADA declara-se ciente e concorda, bem como adotará todas as medidas para deixar seus parceiros, Colaboradores e clientes também cientes, e que a CONTRATADA em decorrência do

presente contrato poderá ter acesso, utilizará, e processará, eletrônica e manualmente, informações e dados prestados pela executora e seus clientes (“Dados Protegidos”).
11.10. As PARTES declaram-se cientes dos direitos, obrigações e penalidades aplicáveis constantes da Lei Geral de Proteção de Dados Pessoais – “LGPD” (Lei 13.709/2018), e obrigam-se a adotar todas as medidas razoáveis par garantir, por si, bem como seu pessoal, colaboradores, empregados e subcontratados que utilizem os Dados Protegidos na extensão autorizada na referida LGPD, nos termos do ANEXO I e II.

CLÁUSULA DÉCIMA SEGUNDA: DAS OBRIGAÇÕES DAS PARTES

12.1. **DO CONTRATANTE:**

12.1.1. Acompanhar a execução de todo o trabalho desenvolvido, assim como questionar quaisquer eventualidades que desvirtuem o seu caráter intrínseco;
12.1.2. Prestar as informações e os esclarecimentos que forem solicitados pela **CONTRATADA** durante o prazo de vigência do Contrato;
12.1.3. Proporcionar todas as facilidades para que a CONTRATADA possa desempenhar seus serviços dentro do especificado neste **CONTRATO**;
12.1.4. Efetuar os pagamentos conforme clausula 4ª do presente contrato;

12.2. **DA CONTRATADA**:

12.2.1. Executar o objeto do presente **CONTRATO** desenvolvendo conteúdos próprios para realização dos módulos e aplicação do conteúdo mediante prévia aprovação do CONTRATANTE;
12.2.2. Prestar serviços dentro dos parâmetros e rotinas estabelecidos, com observância às recomendações aceitas pela boa técnica de procedimentos, das normas que regulamentam o objeto;
12.2.3. Manter absoluto sigilo sobre quaisquer informações de que venha a tomar conhecimento ou ter acesso quando da execução do objeto do presente instrumento;
12.2.4. Arcar com a responsabilidade civil por todos e quaisquer danos materiais e morais causados pela ação ou omissão de seus empregados, trabalhadores, prepostos ou representantes, dolosa ou culposamente, à Contratante.
12.2.5. Cumprir fielmente com o CONTRATO, prestando os serviços com respeito às Leis e garantindo qualidade, pontualidade e zelo no atendimento à Contratante.
12.2.6. Não veicular publicidade ou qualquer outra informação relativa à CONTRATANTE ou aos serviços objeto deste contrato, sem prévia autorização da CONTRATANTE.

CLÁUSULA DÉCIMA TERCEIRA: DA GARANTIA

13.1. A garantia dos equipamentos, software, suporte técnico, instalação e configuração após seu pleno funcionamento será de 90 (noventa) dias e de responsabilidade da contratada, iniciando-se um dia útil após a emissão do Termo de Recebimento Definitivo.
13.2. Durante o período indicado acima, qualquer atividade relacionada ao funcionamento dos produtos, como manutenção evolutiva, preventiva e corretiva, estará incluída na garantia, sem nenhum ônus para o CONTRATANTE. Após este período, a garantia deverá ser realizada pelo fabricante do equipamento.
13.3. A garantia durante o período de 90 (noventa) dias deverá ser prestada pelo profissional indicado pela contratada.

CLÁUSULA DÉCIMA QUARTA: DISPOSIÇÕES FINAIS

14.1. O presente instrumento poderá ser modificado, através de Termos Aditivos, se de comum acordo entre as partes, vedada a alteração da natureza do objeto pactuado neste **CONTRATO**.
14.2. Fica eleito o Foro da Comarca de Belo Horizonte, Estado de Minas Gerais, que será o competente para dirimir dúvidas decorrentes da execução deste **CONTRATO**.

14.3. Caso a CONTRATADA, no decorrer da prestação dos serviços, demonstre inaptidão técnica, operacional ou administrativa, bem como quaisquer outras características que, no entendimento do CONTRATANTE, possa prejudicar, inviabilizar, retardar ou desvirtuar o objetivo pretendido, poderá o CONTRATANTE aplicar as penalidades previstas no presente contrato.
14.4. O não exercício, pelo CONTRATANTE, de qualquer dos direitos previstos neste contrato não constituirá renúncia ou novação, podendo tais direitos e prerrogativas ser por ela exercido a qualquer tempo.
14.5. Casos omissos e modificações serão resolvidos entre as partes através de termos aditivos, que farão parte integrante deste CONTRATO;
14.6. O **CONTRATANTE** poderá introduzir acréscimos ou supressões que se fizerem necessários, em até 50% (cinquenta por cento) do valor inicial do contrato, conforme lhe faculta o artigo 38 do Regulamento de Licitações e Contratos do Sescoop.
14.7. Os casos fortuitos ou de força maior serão excludentes de responsabilidade das partes, na forma do Código Civil Brasileiro.

Como alternativa à assinatura física do Instrumento, as Partes declaram e concordam que as assinaturas mencionadas poderão ser efetuadas em formato eletrônico, sendo a(s) respectiva(s) folha(s) de assinaturas documento integrante e inseparável deste Instrumento Contratual, sob pena de nulidade, declarando ainda e desde já, reconhecerem a veracidade, autenticidade e validade deste Instrumento e de seus termos, incluindo seus anexos, nos termos do art. 219 do Código Civil, por meio de certificados eletrônicos e digitais, nos termos do art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (“MP nº 2.200-2”) e da legislação vigente da autoridade certificadora ICP-Brasil.

E por estarem assim, justas e contratadas, assinam as partes o presente, na presença das testemunhas abaixo, que também o assinam.

Belo Horizonte, XX de julho de 2024.

SESCOOP/MG

ALEXANDRE GATTI LAGES **SUPERINTENDENTE**	**ISABELA CHENNA PEREZ** **GERENTE GERAL**

XXXXXXXXXX

XXXXXXXXXX

TESTEMUNHAS

MOACIR LOURENÇO ROSA JUNIOR	**ROBERT MARTINS SANTOS**