ESTADO DE MINAS GERAIS

SECRETARIA DE ESTADO DE FAZENDA

Diretoria de Aquisições e Contratos/Divisão de Aquisições

Versão v.30.11.2020.

Processo SEI nº 1190.01.0010082/2021-93

EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 1191001 48/2021
PROCESSO DE COMPRA Nº 1191001 48/2021

Fornecimento de Bens com entrega IMEDIATA
Critério de Julgamento: menor preço
Modo de disputa: Aberto

Licitação com participação ampla (sem reserva de lotes para ME e EPP)

Objeto: Aquisição de solução de segurança com funcionalidades de *Firewall*, Sistema de Prevenção de Intrusão (IPS), Redes Virtuais Privadas (VPN), Controle de Aplicações e Ameaças, Filtro de URL e Protocolo de Qualidade de Serviço (QoS) Integrados e servidores para substituição dos equipamentos ora em uso na SEF-MG, assim como serviços de atualização, garantia, instalação, suporte, e treinamento para o ambiente de Data Center, conforme especificações, exigências e quantidades estabelecidas neste Edital e seus Anexos.

EDITAL

1. PREÂMBULO

O ESTADO DE MINAS GERAIS, por intermédio da SECRETARIA DE ESTADO DE FAZENDA DE MINAS GERAIS - SEF/MG torna pública a realização de licitação na modalidade pregão eletrônico do tipo menor preço, no modo de disputa aberto, em sessão pública, por meio do site www.compras.mg.gov.br, visando a aquisição de solução de segurança com funcionalidades de *Firewall*, Sistema de Prevenção de Intrusão (IPS), Redes Virtuais Privadas (VPN), Controle de Aplicações e Ameaças, Filtro de URL e Protocolo de Qualidade de Serviço (QoS) Integrados e servidores para substituição dos equipamentos ora em uso na SEF-MG, assim como serviços de atualização, garantia, instalação, suporte, e treinamento para o ambiente de Data Center, nos termos da Lei Federal n° 10.520, de 17 de Julho de 2002 e da Lei Estadual n°. 14.167, de 10 de Janeiro de 2002 e do Decreto Estadual n° 48.012, de 22 de julho de 2020 .

Este pregão será amparado pela **Lei Complementar** nº. 123, de 14 de dezembro de 2006 e pelas **Leis Estaduais** nº. 13.994, de 18 de setembro de 2001, nº. 20.826, de 31 de julho de 2013, pelos **Decretos Estaduais** nº. 45.902, de 27 de janeiro de 2012, nº 47.437, 26 de junho de 2018, nº Decreto 47.524, de 6 de novembro de 2018, nº. 37.924, de 16 de maio de 1996, pelas **Resoluções SEPLAG** nº. 13, de 07 de fevereiro de 2014 e nº 93, de 28 novembro de 2018, pelas **Resoluções Conjuntas SEPLAG / SEF** n.º 3.458, de 22 de julho de 2003 e nº 8.898 de 14 de junho 2013, pela **Resolução Conjunta SEPLAG/SEF/JUCEMG** n.º 9.576, de 6 de julho 2016, aplicando-se subsidiariamente, a **Lei Federal n° 8.666,** de 21 de Junho de 1993, e as condições estabelecidas nesse edital e seus anexos, que dele constituem parte integrante e inseparável para todos os efeitos legais.

1.1. O pregão será realizado pela Pregoeira Eliana Mara Marcolino - Masp: 363.129-8, designada na Portaria SEF/SPGF n.º 01, de 24 de maio de 2021, e Equipe de Apoio constituída pelos servidores: Izabelle Passos Gouvêa - Masp: 752.556-1 e Sílvio Henrique Araújo Couto - Masp 669.259-4.

1.1.1. Em caso de impossibilidade de comparecimento da pregoeira indicada no item anterior, atuará como sua substituta a Pregoeira Lúcia Helena Tamie Anraki - Masp: 340.144-5, designada por meio da Portaria SEF/SPGF n.º 01, de 24 de maio de 2021.

1.1.2. A sessão de pregão terá início no dia 08 de outubro de 2021, às 9h30min. 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 e na documentação relativa ao certame.

1.2. A sessão de pregão será realizada no sítio eletrônico de compras do Governo do Estado de Minas Gerais: www.compras.mg.gov.br.

2. OBJETO

2.1. A presente licitação tem por objeto a aquisição de solução de segurança com funcionalidades de *Firewall*, Sistema de Prevenção de Intrusão (IPS), Redes Virtuais Privadas (VPN), Controle de Aplicações e Ameaças, Filtro de URL e Protocolo de Qualidade de Serviço (QoS) Integrados e servidores para substituição dos equipamentos ora em uso na SEF-MG, assim como serviços de atualização, garantia, instalação, suporte, e treinamento para o ambiente de Data Center, conforme especificações constantes no Anexo I - Termo de Referência, e de acordo com as exigências e quantidades estabelecidas neste edital e seus anexos.

2.2. Em caso de divergência entre as especificações do objeto descritas no Portal de Compras e as especificações técnicas constantes no Anexo I - Termo de Referência, o licitante deverá obedecer a este último.

3. DO PEDIDO DE ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO

3.1. Os pedidos de esclarecimentos e os registros de impugnações referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico, no site http://www.compras.mg.gov.br/.

3.1.1. Os pedidos de esclarecimento e registros de impugnação serão realizados, em caso de indisponibilidade técnica ou material do sistema oficial do Estado de Minas Gerais, alternativamente, via e-mail spgfdaclicitacao@fazenda.mg.gov.br, observado o prazo previsto no item 3.1.

3.1.2. É obrigação do autor do pedido de esclarecimento ou do registro de impugnação informar à Secretaria de Estado de Fazenda de Minas Gerais a indisponibilidade do sistema.

3.2. O pedido de esclarecimentos ou registro de impugnação pode ser feito por qualquer pessoa no Portal de Compras na página do pregão, em campo próprio (acesso via botão “Esclarecimentos/Impugnação”).

3.2.1. Nos pedidos de esclarecimentos ou registros de impugnação os interessados deverão se identificar (CNPJ, Razão Social e nome do representante que pediu esclarecimentos, se pessoa jurídica e CPF para pessoa física) e disponibilizar as informações para contato (endereço completo, telefone e e-mail).

3.2.2. Podem ser inseridos arquivos anexos com informações e documentações pertinentes as solicitações.

3.2.3. Após o envio da solicitação, as informações não poderão ser mais alteradas, ficando o pedido registrado com número de entrada, tipo (esclarecimento ou impugnação), data de envio e sua situação.

3.2.4. A resposta ao pedido de esclarecimento ou ao registro de impugnação também será disponibilizada via sistema. O solicitante receberá um e-mail de notificação e a situação da solicitação alterar-se-á para “concluída”.

3.3. O pregoeiro responderá no prazo de 02 (dois) dias úteis, contados da data de recebimento, e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos.

3.4. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

3.5. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

3.5.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

3.6. As respostas aos pedidos de impugnações e esclarecimentos aderem a este Edital tal como se dele fizessem parte, vinculando a Administração e os licitantes.

3.7. Qualquer modificação no Edital exige divulgação pelo mesmo instrumento de publicação em que se deu o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

3.8. As denúncias, petições e impugnações anônimas ou não fundamentadas não serão analisadas e serão arquivadas pela autoridade competente.

3.9. A não impugnação do edital, na forma e tempo definidos nesse item, acarreta a decadência do direito de discutir, na esfera administrativa, as regras do certame.

3.10. Na contagem dos prazos estabelecidos neste edital, exclui-se o dia do início e inclui-se o do vencimento, e consideram-se os dias úteis. Só se iniciam e expiram os prazos em dia de expediente na Administração.

4. DAS CONDIÇÕES DE PARTICIPAÇÃO

4.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no termos do Decreto Estadual nº 47.524, de 6 de novembro de 2018 e Resolução SEPLAG nº 93, de 28 de novembro de 2018, no Cadastro Geral de Fornecedores – CAGEF.

4.2. É vedado a qualquer pessoa, física ou jurídica, representar mais de um licitante na presente licitação.

4.3. Para fins do disposto neste edital, o enquadramento dos beneficiários indicados no caput do art. 3º do Decreto Estadual nº 47.437, de 26 de junho de 2018 se dará da seguinte forma:

4.3.1. microempresa ou empresa de pequeno porte, conforme definido nos incisos I e II do caput § 4º do art. 3º da Lei Complementar Federal nº 123, de 14 de dezembro de 2006;

4.3.2. agricultor familiar, conforme definido na Lei Federal nº 11.326, de 24 de julho de 2006;

4.3.3. produtor rural pessoa física, conforme disposto na Lei Federal nº 8.212, de 24 de julho de 1991;

4.3.4. microempreendedor individual, conforme definido no § 1º do art. 18-A da Lei Complementar Federal nº 123, de 14 de dezembro de 2006;

4.3.5. sociedade cooperativa, conforme definido no art. 34 da Lei Federal nº 11.488, de 15 de junho de 2007, e no art. 4º da Lei Federal nº 5.764, de 16 de dezembro de 1971.

4.4. **NÃO PODERÃO PARTICIPAR** as empresas que:

4.4.1. Encontrarem-se em situação de falência, concurso de credores, dissolução, liquidação;

4.4.2. Enquadrarem-se como sociedade estrangeira não autorizada a funcionar no País;

4.4.3. Estiverem suspensas temporariamente de participar de licitações ou impedidas de contratar com a Administração, sancionadas com fundamento no art. 87, III, da Lei Federal nº 8.666, de 21 de junho de 1993;

4.4.4. Estiverem impedidas de licitar e contratar com o Estado de Minas Gerais, sancionadas com fundamento no art. 7º da Lei Federal nº 10.520, de 17 de julho de 2002;

4.4.5. Forem declaradas inidôneas para licitar e contratar coma Administração Pública Federal, Estadual ou Municipal, sancionadas com fundamento no art. 87, IV, da Lei Federal nº 8.666, de 21 de junho de 1993;

4.4.6. Empresas que tenham como proprietários controladores ou diretores membros dos poderes legislativos da União, Estados ou Municípios ou que nelas exerçam funções remuneradas, conforme art. 54, II, "a", c/c art. 29, IX, ambos da Constituição da República;

4.4.7. Estiverem inclusas em uma das situações previstas no art. 9° da Lei Federal nº 8.666, de 21 de junho de 1993;

4.4.8. Empresas reunidas em consórcio.

4.5. A observância das vedações para não participação é de inteira responsabilidade do licitante que se sujeitará às penalidades cabíveis, em caso de descumprimento.

4.6. Como condição para participação no Pregão, a licitante assinalará, no momento de cadastramento de sua proposta, "sim" ou "não" em campo próprio do sistema eletrônico, relativo às seguintes declarações:

4.6.1. que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

4.6.1.1. Alternativamente ao campo disposto no item 4.6.1, que, para fins de obtenção do tratamento diferenciado e simplificado de que trata a Lei Complementar 123, de 14 de dezembro de 2006 e o artigo 15 da Lei Estadual 20.826, de 31 de julho de 2013, registra que possui restrição no (s) documento (s) de regularidade fiscal, com o compromisso de que irá promover a sua regularização caso venha a formular o lance vencedor, cumprindo plenamente os demais requisitos de habilitação, conforme determina o inciso XIII do art. 9º da Lei Estadual nº 14.167/2002.

4.6.2. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

4.7. Além das declarações prestadas via sistema, o licitante deverá anexar, juntamente com a documentação de habilitação, as seguintes declarações constantes do anexo IV do Edital:

4.7.1. que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, quando for o caso;

4.7.2. que está ciente das condições contidas no Edital e seus anexos;

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

4.7.4. que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

5. DO CREDENCIAMENTO

5.1. Para acesso ao sistema eletrônico o fornecedor deverá credenciar-se, nos termos do Decreto Estadual nº 47.524, de 6 de novembro de 2018 e Resolução SEPLAG nº 93, de 28 de novembro de 2018, por meio do site **www.compras.mg.gov.br**, na opção **Cadastro de Fornecedores**, no prazo mínimo de 02 (dois) dias úteis antes da data da sessão do Pregão.

5.1.1. Cada fornecedor deverá credenciar, no mínimo, um representante para atuar em seu nome no sistema, sendo que o representante receberá uma senha eletrônica de acesso.

5.2. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

5.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no CAGEF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

5.3.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

5.4. O fornecimento da senha é de caráter pessoal e intransferível, sendo de inteira responsabilidade do fornecedor e de cada representante qualquer transação efetuada, não podendo ser atribuídos ao provedor ou ao gestor do sistema eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

5.4.1. O fornecedor se responsabiliza por todas as transações realizadas em seu nome, assumindo como firmes e verdadeiras as propostas e os lances efetuados por seu representante, sendo que o credenciamento do representante do fornecedor implicará responsabilidade pelos atos praticados e a presunção de capacidade técnica para a realização das transações, sob pena da aplicação de penalidades.

5.5. Informações complementares a respeito do cadastramento serão obtidas no *site* **www.compras.mg.gov.br** ou pela Central de Atendimento aos Fornecedores, via e- mail: cadastro.fornecedores@planejamento.mg.gov.br, com horário de atendimento de Segunda-feira à Sexta-feira das 08:00h às 16:00h.

5.6. O fornecedor enquadrado dentre aqueles listados no subitem 5.3 que desejar obter os benefícios previstos no Capítulo V da Lei Complementar Federal nº 123, de 14 de dezembro de 2006, disciplinados no Decreto Estadual nº.47.437, de 2018 e pela Resolução Conjunta SEPLAG/SEF/JUCEMG nº 9.576, de 6 de julho de 2016, deverá comprovar a condição de beneficiário no momento do seu credenciamento ou quando da atualização de seus dados cadastrais no Cadastro Geral de Fornecedores – CAGEF, desde que ocorram em momento anterior ao cadastramento da proposta comercial.

5.6.1. Não havendo comprovação, no CAGEF, da condição de beneficiário até o momento do registro de proposta, o fornecedor não fará jus aos benefícios lista dos no Decreto Estadual nº 47.437, de 26 de junho de 2018.

6. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

6.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

6.1.1. Os arquivos referentes à proposta comercial e à documentação de habilitação deverão ser anexados no sistema, por upload, separadamente em campos próprios.

6.1.1.1. Os arquivos referentes à proposta comercial e os documentos de habilitação deverão ser assinados eletronicamente.

6.1.1.1.1. Para assinatura eletrônica, poderá ser utilizado o Portal de Assinatura Digital disponibilizado pelo Governo de Minas Gerais, de acesso gratuito, disponível em:

http://www.portaldeassinaturas.mg.gov.br. Dúvidas com relação à utilização do Portal de Assinaturas Digital podem ser encaminhadas para o e-mail comprascentrais@planejamento.mg.gov.br. A realização da assinatura digital importará na aceitação de todos os termos e condições que regem o processo eletrônico, conforme Decreto nº 47.222, de 26 de julho de 2017, e demais normas aplicáveis, admitindo como válida a assinatura eletrônica, tendo como consequência a responsabilidade pelo uso indevido das ações efetuadas e das informações prestadas, as quais serão passíveis de apuração civil, penal e administrativa.

6.1.2. As orientações para cadastro de proposta e envio dos documentos de habilitação encontram-se detalhadas no Manual Pregão Eletrônico - Decreto nº 48.012/2020 acessível pelo Portal de Compras.

6.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

6.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do Certificado de Registro Cadastral emitido pelo CAGEF, cuja consulta é pública. Nesse caso os licitantes assinalarão em campo próprio no sistema a opção por utilizar a documentação registrada no CAGEF, não sendo necessário o envio dos documentos que estiverem vigentes.

6.4. Os documentos que constarem vencidos no CAGEF e os demais documentos exigidos para a habilitação, que não constem do CAGEF, deverão ser anexados em até 5 arquivos de 20 Mb cada.

6.5. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da Lei Complementar nº 123/2006.

6.6. Incumbirá ao 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.

6.7. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

6.8. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

6.9. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

6.10. O prazo de validade da proposta será de 60 (sessenta) dias contados da data de abertura da sessão pública estabelecida no preâmbulo deste Edital e seus anexos, podendo substituí-la ou retirá-la até a abertura da sessão.

7. DO PREENCHIMENTO DA PROPOSTA

7.1. O licitante deverá encaminhar sua proposta, mediante o preenchimento, no sistema eletrônico, dos campos abaixo, bem como, realizar o upload sua proposta comercial, conforme modelo constante no Anexo III - Proposta Comercial.

7.1.1. Valor unitário e total;

7.1.2. Marca;

7.1.3. Modelo;

7.1.4. Anexar em PDF arquivo referente à Proposta Comercial

contendo especificações do objeto, bem como outras informações pertinentes presentes no Anexo I- Termo de Referência;

7.1.5. Devem ser anexadas informações para a avaliação da proposta inicial constante de folder, catálogo, ficha para os seguintes lotes 1 e 2.

7.1.6. O preenchimento dos campos do sistema bem como o arquivo referente a Proposta Comercial anexada deverá se referir, individualmente, a cada lote.

7.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

7.3. Nos preços propostos deverão estar incluídos todos os tributos, encargos sociais, financeiros e trabalhistas, taxas e quaisquer outros ônus que porventura possam recair sobre a execução do objeto da presente licitação, os quais ficarão a cargo única e exclusivamente da CONTRATADA.

7.3.1. Todos os preços ofertados deverão ser apresentados em moeda corrente nacional, em algarismos com duas casas decimais após a vírgula.

7.4. Os fornecedores estabelecidos no Estado de Minas Gerais que forem isentos do ICMS, conforme dispõe o Decreto nº 43.080, de 2002, deverão informar na proposta, conforme anexo presente no Portal de Compras, os valores com e sem ICMS que serão classificados conforme itens abaixo.

7.4.1. Os fornecedores mineiros deverão informar nas propostas enviadas, pelo sistema eletrônico, as informações relativas ao produto e ao preço resultante da dedução do ICMS, conforme Resolução conjunta SEPLAG/SEF nº 3.458, de 22 de julho de 2003, alterada pela Resolução conjunta SEPLAG/SEF nº 4.670, de 5 de junho de 2014.

7.4.2. A classificação das propostas, etapa de lances, o julgamento dos preços e a homologação serão realizados a partir dos preços dos quais foram deduzidos os valores relativos ao ICMS.

7.4.3. Os fornecedores mineiros não optantes pelo Simples Nacional farão suas propostas conforme as disposições contidas nos subitens 7.4.1. e 7.4.2.

7.4.4. O disposto nos subitens 7.4.1. e 7.4.2 não se aplica aos contribuintes mineiros optantes pelo regime do Simples Nacional.

7.4.5. Os fornecedores mineiros de que trata o subitem 7.4.4 deverão anexar às suas propostas comerciais a ficha de inscrição estadual, na qual conste a opção pelo Simples Nacional, podendo o pregoeiro, na sua falta, consultar a opção por este regime através do site: http://www8.receita.fazenda.gov.br/SimplesNacional/.

7.4.6. O fornecedor mineiro isento de ICMS , caso seja vencedor, deverá enviar, quando solicitado pelo Pregoeiro, via chat, após a negociação, sua proposta comercial assinada e atualizada com os valores finais ofertados durante a sessão deste Pregão, informando na proposta, além do preço resultante da dedução do ICMS, o preço com ICMS.

8. DA SESSÃO DO PREGÃO E DO JULGAMENTO

8.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

8.2. O Pregoeiro verificará as propostas apresentadas, preservado o sigilo do licitante, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

8.2.1. A análise da proposta que trata o item anterior é uma análise prévia, e não poderá implicar quebra de sigilo do fornecedor, bem como não exime a Administração da verificação de sua conformidade com todas as

especificações contidas neste edital e seus anexos, quando da fase de aceitabilidade da proposta do licitante detentor do menor preço para cada lote.

8.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

8.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

8.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

8.3.1. Durante o transcurso da sessão pública, serão divulgados, em tempo real, o valor e horário do menor lance apresentado pelos licitantes, bem como todas as mensagens trocadas no "chat" do sistema, sendo vedada a identificação do fornecedor.

8.3.2. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

8.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

8.4.1. O lance deverá ser ofertado pelo valor total para cada lote.

8.5. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

8.6. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

8.7. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$800,00 (oitocentos reais) para o **Lote 01** e de R$400,00 (quatrocentos reais) para o **Lotes 02**.

8.8. Será adotado para o envio de lances no pregão eletrônico o modo de disputa "aberto", em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

8.9. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da etapa competitiva.

8.10. A prorrogação automática da etapa de envio de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive em lances intermediários.

8.11. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública será encerrada automaticamente.

8.12. Encerrada a fase competitiva sem prorrogação automática pelo sistema, nos temos do subitem 7.9., o pregoeiro poderá admitir o reinício da etapa de envio de lances, em prol da consecução do melhor preço.

8.13. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

8.14. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

8.15. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

8.16. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e

reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

8.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

8.18. **Do empate ficto**

8.18.1. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação junto ao CAGEF do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto Estadual nº 47.437/2018.

8.18.2. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

8.18.2.1. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

8.18.2.2. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

8.18.2.3. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

8.19. **Do empate real**

8.19.1. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

8.19.2. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:

8.19.2.1. no país;

8.19.2.2. por empresas brasileiras;

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

8.19.2.4. por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

8.19.3. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas ou os lances empatados.

8.20. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, via chat, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta,

vedada a negociação em condições diferentes das previstas neste Edital.

8.20.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

8.20.2. O pregoeiro solicitará ao licitante melhor classificado que, no prazo de 02 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

8.21. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

8.22. **DA ACEITABILIDADE DA PROPOSTA VENCEDORA**

8.22.1. O critério de julgamento será o de **MENOR PREÇO GLOBAL OFERTADO POR LOTE**, apurado de acordo com o Anexo III - Proposta Comercial.

8.22.2. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao valor estimado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 48.012/2020.

8.22.2.1. Será desclassificada a proposta ou o lance vencedor, para todos os fins aqui dispostos, que não atender às exigências fixadas neste Edital, contenha vícios insanáveis, manifesta ilegalidade ou apresentar preços manifestamente inexequíveis.

8.22.2.2. Considera-se inexequível a proposta que apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

8.22.2.2.1. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 para que a empresa comprove a exequibilidade da proposta.

8.22.3. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita;

8.22.4. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata;

8.22.5. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade de diligência disponível no sistema, no prazo de no prazo de 02 (duas) horas, sob pena de não aceitação da proposta.

8.22.5.1. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

8.22.5.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro,

sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

8.22.6. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

8.22.7. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a sua continuidade.

8.22.7.1. Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

8.22.8. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

9. DA APRESENTAÇÃO DE AMOSTRAS

9.1. Não haverá apresentação de amostras no presente certame.

10. DA VERIFICAÇÃO DA HABILITAÇÃO

10.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) CADIN – Cadastro Informativo de Inadimplência em relação à Administração Pública do Estado de Minas Gerais acessível pelo site http://consultapublica.fazenda.mg.gov.br/ConsultaPublicaCADIN/consultaSituacaoPublica.do;

b) CAGEF/CAFIMP – Cadastro de Fornecedores Impedidos acessível pelo site https://www.fornecedores2.mg.gov.br/portalcompras/fornecedoresimpedidoscon.do;

c) Lista de Inidôneos mantidos pelo Tribunal de Contas da União - TCU; https://certidoes-apf.apps.tcu.gov.br/;

10.1.1. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário. https://www.cnj.jus.br/improbidade_adm/consultar_requerido.php.

10.1.1.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

10.1.1.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

10.1.1.3. O licitante será convocado para manifestação previamente à sua inabilitação.

10.1.2. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

10.1.3. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

10.2. Caso atendidas as condições de participação, a habilitação dos licitantes será verificada por meio do CAGEF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação

econômica financeira e habilitação técnica, conforme o disposto no Decreto nº 47.524/2018.

10.2.1. O interessado, para efeitos de habilitação prevista nesse edital mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no CAGEF até (2) dias úteis anteriores à data prevista para recebimento das propostas;

10.2.2. É dever do licitante atualizar previamente as comprovações constantes do CAGEF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

10.2.2.1. Caso as comprovações constantes do CAGEF vençam entre a data de envio da documentação concomitante ao cadastro da proposta e o momento da verificação da habilitação, deverá ser solicitado pelo pregoeiro ao licitante o envio da documentação atualizada, por meio de documentação complementar via sistema.

10.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 48.012/20.

10.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de no prazo de 02 (duas) horas, sob pena de inabilitação.

10.4. A apresentação de documentos físicos originais somente será exigida se houver dúvida quanto à integridade do arquivo digitalizado.

10.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.6. Ressalvado o disposto no item 6.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação.

10.7. **HABILITAÇÃO JURÍDICA**

10.7.1. Documento de identificação, com foto, do responsável pelas assinaturas das propostas comerciais constantes no Anexo III - Proposta Comercial e das declarações constantes no Anexo IV - Modelos de Declarações.

10.7.1.1. Se for o caso, apresentar procuração conferindo poderes ao(s) responsável(is) pela empresa para praticar atos junto à Administração Pública.

10.7.2. Registro empresarial na Junta Comercial, no caso de empresário individual;

10.7.3. Ato constitutivo, estatuto ou contrato social e suas alterações posteriores ou instrumento consolidado, devidamente registrado na Junta Comercial, em se tratando de sociedades empresárias, cooperativas ou empresas individuais de responsabilidade limitada e, no caso de sociedade de ações, acompanhado de documentos de eleição ou designação de seus administradores;

10.7.4. Ato constitutivo devidamente registrado no Registro Civil de Pessoas Jurídicas em se tratando de sociedade não empresária, acompanhado de prova da diretoria em exercício;

10.7.5. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País.

10.7.6. Ato de registro ou autorização para funcionamento expedido pelo Órgão competente, quando a atividade assim o exigir;

10.7.7. Os documentos acima deverão estar acompanhados de todas

as alterações ou da consolidação respectiva;

10.8. **REGULARIDADE FISCAL E TRABALHISTA**

10.8.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda -CNPJ;

10.8.2. Prova de inscrição no Cadastro de Contribuintes Estadual ou Municipal, relativo à sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame;

10.8.3. Prova de regularidade perante as Fazendas Federal, Estadual sede do licitante, Municipal e perante a Fazenda Estadual de MG;

10.8.3.1. A prova de regularidade fiscal e seguridade social perante a Fazenda Nacional será efetuada mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil – RFB e pela Procuradoria-Geral da Fazenda Nacional – PGFN, referente a todos os tributos federais e à Dívida Ativa da União – DAU por elas administrados, bem como das contribuições previdenciárias e de terceiros.

10.8.3.2. Se o fornecedor não estiver inscrito no cadastro de contribuintes do Estado de Minas Gerais deverá comprovar a inexistência de débitos relativos a tributos estaduais em Minas Gerais por meio de Certidão de Débito Tributário – CDT, que poderá ser emitida pelo site www.fazenda.mg.gov.br.

10.8.4. Certificado de Regularidade relativa à seguridade social e perante o Fundo de Garantia por Tempo de Serviço –FGTS.

10.8.5. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa, ou positiva com efeito de negativa, nos termos da Lei Federal nº 12.440, de 7 de julho de 2011, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

10.8.6. A comprovação da regularidade fiscal e/ou trabalhista deverá ser efetuada mediante a apresentação das competentes certidões negativas de débitos, ou positivas com efeitos de negativas.

10.8.7. Caso o fornecedor seja considerado isento dos tributos estaduais relacionados ao objeto licitado, deverá comprovar tal condição mediante a apresentação de declaração do domicílio ou sede do fornecedor, ou outra equivalente, na forma da lei.

10.9. **QUALIFICAÇÃO ECONÔMICO-FINANCEIRA**

10.9.1. Certidão negativa de falência expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida pelo distribuidor do domicílio da pessoa física, emitida nos últimos 06 (seis) meses;

10.10. **QUALIFICAÇÃO TÉCNICA:**

10.10.1. Comprovação de aptidão para efetuar o fornecimento compatível com as características e quantidades do objeto da licitação, estabelecidas no Termo de Referência ANEXO a este Edital, por meio da apresentação de atestados de desempenho anterior, fornecidos por pessoa jurídica de direito público ou privado,comprobatório da capacidade técnica para atendimento ao objeto da presente licitação, vedado o auto atestado, compreendendo os requisitos abaixo relacionados:

10.10.1.1. **Lote 01 e Lote 2:** Atestado(s) de Capacidade Técnica da licitante, emitido(s) por entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou empresa privada que comprove, de maneira satisfatória, a aptidão para desempenho de atividades pertinentes ao objeto a ser licitado, comprovando o fornecimento prévio de produtos e/ou serviços similares aos especificados no objeto desta aquisição, contemplando garantias compatíveis às exigidas em relação a prazos, níveis de serviços e características.

10.10.2. Os atestados deverão conter:

10.10.2.1. Nome empresarial e dados de identificação da instituição emitente (CNPJ, endereço, telefone).

10.10.2.2. Local e data de emissão.

10.10.2.3. Nome, cargo, telefone, e-mail e a assinatura do responsável pela veracidade das informações.

10.10.3. Para atendimento do quantitativo indicado nos subitens do item 10.10.1, é admitido o somatório de atestados, desde que compatíveis com as características do objeto da licitação.

10.10.3.1. O licitante deve disponibilizar, quando solicitado pelo pregoeiro, todas as informações necessárias à comprovação da legitimidade dos atestados solicitados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da CONTRATANTE e local em que foram executadas as atividades.

10.11. DA PARTICIPAÇÃO DE CONSÓRCIOS

10.11.1. Não será permitida a participação de empresas reunidas em consórcio, devido à baixa complexidade do objeto a ser adquirido, considerando que as empresas que atuam no mercado têm condições de prestar os serviços de forma independente.

10.12. **DISPOSIÇÕES GERAIS DA HABILITAÇÃO:**

10.12.1. O licitante que possuir o Certificado de Registro Cadastral (CRC) emitido pela Unidade Cadastradora da Secretaria de Estado de Planejamento e Gestão – SEPLAG poderá utilizá-lo como substituto de documento dele constante, exigido para este certame, desde que este esteja com a validade em vigor no CRC. Caso o documento constante no CRC esteja com a validade expirada, tal não poderá ser utilizado, devendo ser apresentado documento novo com a validade em vigor.

10.12.1.1. Serão analisados no CRC somente os documentos exigidos para este certame, sendo desconsiderados todos os outros documentos do CRC, mesmo que estejam com a validade expirada.

10.12.2. Os documentos exigidos para habilitação serão apresentados no momento do cadastramento da proposta, conforme instruções do Portal de Compras http://www.compras.mg.gov.br/, e serão analisados após a classificação das propostas.

10.12.2.1. Para fins de habilitação, é facultada ao pregoeiro a verificação de informações e o fornecimento de documentos que constem de sítios eletrônicos de órgãos e entidades das esferas municipal, estadual e federal, emissores de certidões, devendo tais documentos ser juntados ao processo.A Administração não se responsabilizará pela eventual indisponibilidade dos meios eletrônicos, no momento da verificação. Ocorrendo essa indisponibilidade e não sendo apresentados os documentos necessários para verificação, o licitante será inabilitado.

10.12.3. Todos os documentos apresentados para a habilitação deverão conter, de forma clara e visível, o nome empresarial, o endereço e o CNPJ do fornecedor.

10.12.3.1. Se o fornecedor figurar como estabelecimento matriz, todos os documentos deverão estar em nome da matriz;

10.12.3.2. Se o fornecedor figurar como filial, todos os documentos deverão estar no nome da filial;

10.12.3.3. Na hipótese de filial, podem ser apresentados documentos que, pela própria natureza, comprovadamente são emitidos em nome da matriz;

10.12.3.4. Em qualquer dos casos, atestados de capacidade técnica ou de responsabilidade técnica podem ser apresentados em nome e com o número do CNPJ(MF) da matriz ou da filial da empresa licitante.

10.12.4. O não atendimento de qualquer das condições aqui previstas provocará a inabilitação do licitante vencedor, sujeitando-o, eventualmente, às punições legais cabíveis.

10.12.5. Aos beneficiários listados no item 5.3 será concedido prazo de 05 (cinco) dias úteis, prorrogáveis por igual período, a critério da administração, para regularização da documentação fiscal e/ou trabalhista, contado a partir da divulgação da análise dos documentos de habilitação do licitante melhor classificado, conforme disposto no inciso I, do § 2º, do art. 6º do Decreto Estadual nº 47.437, de 26 de junho de 2018.

10.12.5.1. A não regularização da documentação no prazo deste item implicará a inabilitação do licitante vencedor, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

10.12.5.2. Se houver a necessidade de abertura do prazo para o beneficiário regularizar sua documentação fiscal e/ou trabalhista, o pregoeiro deverá suspender a sessão de pregão para o lote específico e registrar no "*chat*" que todos os presentes ficam, desde logo, intimados a comparecer no dia e horário informados no site www.compras.mg.gov.br para a retomada da sessão de pregão do lote em referência.

11. DOS RECURSOS

11.1. Declarado o vencedor e decorrida a fase de regularização fiscal e trabalhista da licitante qualificada como microempresa ou empresa de pequeno porte, se for o caso, será concedido o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

11.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

11.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

11.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

11.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias úteis para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias úteis, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.2.4. A apresentação de documentos complementares, em caso de indisponibilidade ou inviabilidade técnica ou material da via eletrônica, devidamente identificados, relativos aos recursos interpostos ou contrarrazões, se houver, será efetuada mediante envio para o e-mail spgfdaclicitacao@fazenda.mg.gov.br, e identificados com os dados da empresa licitante e do processo licitatório (nº. do processo e lote), observado o prazo previsto no item 11.1.

11.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

11.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12. DA REABERTURA DA SESSÃO PÚBLICA

12.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

12.1.1. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.1.2. A convocação se dará por meio do sistema eletrônico (“chat”), e-mail, de acordo com a fase do procedimento licitatório.

12.1.3. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no CAGEF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

13.1. Constatado o atendimento pleno às exigências editalícias, o pregoeiro declarará o licitante vencedor e o sistema gerará ata circunstanciada da sessão, na qual serão registrados todos os atos do procedimento e as ocorrências relevantes, disponível para consulta no site www.compras.mg.gov.br.

13.2. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

13.3. Decididos os recursos porventura interpostos e constatada a regularidade dos atos procedimentais pela autoridade competente, esta adjudicará o objeto ao licitante vencedor e homologará o procedimento licitatório.

14. DA CONTRATAÇÃO

14.1. Encerrado o procedimento licitatório, o representante legal do licitante declarado vencedor será convocado para firmar o termo de contrato, aceitar ou retirar o instrumento equivalente, conforme minuta do Anexo V Contrato, de acordo com o art. 62 da Lei Federal nº 8.666, de 21 de junho de 1993 e Lei Federal nº 10.520, de 17 de julho de 2002.

14.1.1. O instrumento de contratação, e demais atos firmados com a Administração, serão assinados de maneira eletrônica, por intermédio do Sistema Eletrônico de Informações do Governo do Estado de Minas Gerais - SEI/MG.

14.1.1.1. Para a assinatura eletrônica, caso ainda não possua cadastro, o(s) licitante(s) interessado(s) deverá (ão) acessar o Sistema Eletrônico de Informações do Governo do Estado de Minas Gerais - SEI/MG, por meio do link www.sei.mg.gov.br/usuarioexterno, e clicar em "Clique aqui se você ainda não está cadastrado".

14.1.1.2. Dúvidas com relação ao cadastro no SEI podem ser encaminhadas para o e-mail atendimentosei@planejamento.mg.gov.br.

14.1.1.3. A realização do cadastro como Usuário Externo no SEI/MG importará na aceitação de todos os termos e condições que regem o processo eletrônico, conforme Decreto Estadual nº 47.222, de 26 de julho de 2017, e demais normas aplicáveis, admitindo como válida a assinatura eletrônica na modalidade cadastrada (login/senha), tendo como consequência a responsabilidade pelo uso indevido das ações efetuadas e das informações prestadas, as quais serão

passíveis de apuração civil, penal e administrativa.

14.1.2. O adjudicatário deverá comprovar a manutenção das condições de habilitação para firmar o termo de contrato, aceitar ou retirar o instrumento equivalente.

14.1.3. Caso o adjudicatário não apresente situação regular no momento de assinar o termo de contrato, aceitar ou retirar o instrumento equivalente ou recuse-se a assiná-lo, serão convocados os licitantes remanescentes, observada a ordem de classificação.

14.1.3.1. Feita a negociação e comprovados os requisitos de habilitação, o licitante deverá firmar o termo de contrato, aceitar ou retirar o instrumento equivalente, sem prejuízo das sanções previstas no Edital e das demais cominações legais, conforme disposto no art. 48, §2º do Decreto Estadual nº 48.012, de 22 de julho de 2020.

14.2. O representante legal do licitante que tiver apresentado a proposta vencedora deverá firmar o termo de contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo máximo de 5 (cinco) dias úteis a contar do recebimento da comunicação, que se dará através do sistema do Portal de Compras - http://www.compras.mg.gov.br/.

14.3. Qualquer solicitação de prorrogação de prazo para firmar o termo de contrato, aceitar ou retirar o instrumento equivalente decorrentes desta licitação, somente será analisada se apresentada antes do decurso do prazo para tal e devidamente fundamentada.

15. DA SUBCONTRATAÇÃO

15.1. A CONTRATADA, na execução do contrato, sem prejuízo das responsabilidades contratuais e legais, poderá subcontratar parte do objeto conforme discriminado no Anexo I - Termo de Referência.

15.2. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da CONTRATADA pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante o CONTRATANTE pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

16. DA GARANTIA DA EXECUÇÃO

16.1. No que se refere ao item 2 do Lote 1, a CONTRATADA, no prazo máximo de 10 (dez) dias após a assinatura do Contrato, prestará garantia no valor correspondente a 5% do valor do total referente ao item 2 do Lote 1, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 56 da Lei Federal nº 8.666, de 21 de junho de 1993, desde que cumpridas as obrigações contratuais.

16.2. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de mais 03 (três) meses após o término da vigência contratual.

16.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

16.3.1. prejuízos advindos do não cumprimento do objeto do contrato;

16.3.2. prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

16.3.3. multas moratórias e punitivas aplicadas pela Administração à CONTRATADA; e

16.3.4. obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber.

16.4. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

16.5. A garantia em dinheiro deverá ser efetuada em banco oficial em conta específica com correção monetária, em favor do CONTRATANTE;

16.6. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

16.7. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

16.8. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

16.9. Será considerada extinta a garantia:

16.9.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato;

16.9.2. no prazo de 03 meses após o término da vigência, caso a CONTRATANTE não comunique a ocorrência de sinistros.

17. DO PAGAMENTO

17.1. Para os Órgãos/Entidades da Administração Direta ou Indireta do Estado de Minas Gerais, o pagamento será efetuado através do Sistema Integrado de Administração Financeira - SIAFI/MG, por meio de ordem bancária emitida por processamento eletrônico, a crédito do beneficiário em um dos bancos que o fornecedor indicar, no prazo de 30 (trinta) dias corridos da data do recebimento definitivo, com base nos documentos fiscais devidamente conferidos e aprovados pela CONTRATANTE.

17.1.1. Para efeito de pagamento, a CONTRATADA encaminhará à CONTRATANTE, após a execução do objeto, a respectiva nota fiscal/fatura, acompanhada do relatório da execução do objeto do período a que o pagamento se referir, bem como, demais documentos necessários para a efetiva comprovação da execução do objeto, se houver.

17.1.2. A Administração receberá o Documento Auxiliar da Nota Fiscal Eletrônica (DANFE) juntamente com o objeto e deverá realizar a verificação da validade da assinatura digital e a autenticidade do arquivo digital da NF-e (o destinatário tem à disposição o aplicativo “visualizador”, desenvolvido pela Receita Federal do Brasil) e a concessão da Autorização de Uso da NF-e, mediante consulta eletrônica à Secretaria da Fazenda o Portal Nacional daNF-e.

17.1.3. O pagamento da Nota Fiscal fica vinculado à prévia conferência pelo gestor.

17.1.4. As Notas Fiscais que apresentarem incorreções serão devolvidas à CONTRATADA e o prazo para o pagamento passará a correr a partir da data da reapresentação do documento considerado válido pela CONTRATANTE.

17.1.5. Ocorrendo atraso de pagamento por culpa exclusiva da Administração, o valor devido será atualizado financeiramente, entre as datas do vencimento e do efetivo pagamento, de acordo com a variação do Sistema Especial de Liquidação e Custódia –SELIC.

17.2. A CONTRATADA deve garantir a manutenção dos requisitos de habilitação previstos no Edital.

17.3. Eventuais situações de irregularidades fiscal ou trabalhista da CONTRATADA não impedem o pagamento, se o objeto tiver sido executado e atestado. Tal hipótese ensejará, entretanto, a adoção das providências tendentes ao sancionamento da empresa e rescisão contratual.

17.4. Para fins de pagamento, o fornecedor deverá informar domicílio bancário junto ao Banco do Brasil S.A., nos termos da Portaria nº 001, de 9/11/2010, do Diretor da Superintendência Central de Administração Financeira da Secretaria de Estado de Fazenda de Minas Gerais – SCAF/SEF.

17.4.1. Caso o fornecedor não tenha conta no banco a que se refere o subitem 17.4, deverá providenciar a abertura de conta corrente em qualquer agência do referido banco, comunicando à SEF/MG os dados de seu domicílio bancário para fins de certificação de cadastro junto ao Sistema Integrado de Administração Financeira – SIAFI/MG e posterior recebimento de seus créditos.

17.4.2. Excepcionalmente, mediante manifestação formal do fornecedor que esteja impossibilitado de manter conta corrente junto ao Banco do Brasil S.A., o pagamento poderá ser feito nos termos do § 2º do art. 1º da Portaria SCAF nº 001/2010.

18. DAS SANÇÕES ADMINISTRATIVAS

18.1. A licitante/adjudicatária que cometer qualquer das infrações, previstas na Lei Federal nº 8.666, de 21 de junho de 1993, na Lei Federal nº 10.520, de 17 de julho de 2002, Lei Estadual n.º 14.167, de 10 de janeiro de 2002 e no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, e no do Decreto nº 48.012, de 22 de julho de 2020, ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

18.1.1. Advertência por escrito;

18.1.2. Multa de até 20% (vinte por cento) sobre o valor estimado do(s) lote(s) dos quais o licitante tenha participado e cometido a infração;

18.1.3. Suspensão do direito de participar de licitações e impedimento de contratar com a Administração, pelo prazo de até 2 (dois)anos;

18.1.4. Impedimento de licitar e contratar com a Administração Pública Estadual, nos termos do art. 7º da Lei Federal nº 10.520, de 17 de julho de 2002;

18.1.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública;

18.2. A sanção de multa poderá ser aplicada cumulativamente às demais sanções previstas nos itens 18.1.1, 18.1.3, 18.1.4 e 18.1.5.

18.3. A multa será descontada da garantia do contrato, quando houver, e/ou de pagamentos eventualmente devidos ao infrator e/ou cobrada administrativa e/ou judicialmente.

18.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo incidental apensado ao processo licitatório ou ao processo de execução contratual originário que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, bem como o disposto na Lei Federal nº 8.666, de 21 de junho de 1993 e Lei Estadual nº 14.184, de 31 de janeiro de 2002.

18.5. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

18.5.1. Não serão aplicadas sanções administrativas na ocorrência de casos fortuitos, força maior ou razões de interesse público, devidamente comprovados.

18.6. A aplicação de sanções administrativas não reduz nem isenta a obrigação da CONTRATADA de indenizar integralmente eventuais danos causados a Administração ou a terceiros, que poderão ser apurados no mesmo processo administrativo sancionatório.

18.7. As sanções relacionadas nos itens 18.1.3 a 18.1.5 serão obrigatoriamente registradas no Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual –CAFIMP e no CAGEF.

18.8. As sanções de suspensão do direito de participar em licitações e impedimento de licitar e contratar com a Administração Pública poderão ser também aplicadas àqueles que:

18.8.1. Retardarem a execução do objeto;

18.8.2. Comportar-se de modo inidôneo;

18.8.2.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances;

18.8.3. Apresentarem documentação falsa ou cometerem fraude fiscal.

18.9. Durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei Federal nº 12.846, de 1º de agosto de 2013, e pelo Decreto Estadual nº 46.782, de 23 de junho de 2015, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à Controladoria-Geral do Estado, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização –PAR.

19. DISPOSIÇÕES GERAIS

19.1. Este edital deverá ser lido e interpretado na íntegra, e após encaminhamento da proposta não serão aceitas alegações de desconhecimento.

19.2. É facultado ao Pregoeiro ou à Autoridade Superior, em qualquer fase do julgamento, promover diligência destinada a esclarecer ou complementar a instrução do processo e a aferição do ofertado, bem como solicitar a elaboração de pareceres técnicos destinados a fundamentar as decisões.

19.3. O objeto desta licitação deverá ser executado em conformidade com o Anexo I - Termo de Referência, correndo por conta da CONTRATADA as despesas de seguros, transporte, tributos, encargos trabalhistas e previdenciários decorrentes da execução do objeto da contratação.

19.4. É vedado ao licitante retirar sua proposta ou parte dela após aberta a sessão do pregão.

19.5. O pregoeiro, no julgamento das propostas e da habilitação, poderá relevar omissões puramente formais e sanar erros ou falhas que não alterem a substância das propostas, dos documentos e de sua validade jurídica, mediante despacho fundamentado, acessível a todos os interessados, sendo possível a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo.

19.6. A CONTRATADA será constantemente avaliada em termos de suas entregas por procedimentos e critérios definidos no Anexo VII - Avaliação de fornecedores.

19.6.1. Os órgãos e entidades contratantes pertencentes ao Poder Executivo Estadual, dependentes de recursos do Tesouro Estadual, deverão observar o disposto na Resolução SEPLAG nº 13, de 2014.

19.7. A presente licitação somente poderá ser revogada por razão de interesse público decorrente de fato superveniente devidamente comprovado, ou anulada, no todo ou em parte, por ilegalidade, de ofício ou por provocação de

terceiros, mediante parecer escrito e devidamente fundamentado.

19.8. Fica eleito o foro da Comarca de Belo Horizonte, Estado de Minas Gerais, para dirimir eventuais conflitos de interesses decorrentes desta licitação, valendo esta cláusula como renúncia expressa a qualquer outro foro, por mais privilegiado que seja ou venha a ser.

19.9. Os interessados poderão examinar ou retirar gratuitamente o presente Edital de Licitação e seus anexos no site www.compras.mg.gov.br.

ARILSON LEANDRO FERNANDES CORREA LOPES
Diretor de Aquisições e Contratos

BLENDA ROSA PEREIRA COUTO
Superintendente de Planejamento, Gestão e Finanças

Documento assinado eletronicamente por **Blenda Rosa Pereira Couto**, **Superintendente**, em 22/09/2021, às 16:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Arilson Leandro Fernandes Correa Lopes**, **Diretor**, em 23/09/2021, às 10:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **34217107** e o código CRC **9754510B**.

Referência: Processo nº 1190.01.0010082/2021-93 SEI nº 34217107

ESTADO DE MINAS GERAIS

SECRETARIA DE ESTADO DE FAZENDA

Diretoria de Aquisições e Contratos/Divisão de Aquisições

Versão v.20.09.2020.

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO:

O presente Termo de Referência tem por objeto a aquisição de solução de segurança com funcionalidades de *Firewall*, Sistema de Prevenção de Intrusão (IPS), Redes Virtuais Privadas (VPN), Controle de Aplicações e Ameaças, Filtro de URL e Protocolo de Qualidade de Serviço (QoS) Integrados e servidores para substituição dos equipamentos ora em uso na SEF-MG, assim como serviços de atualização, garantia, instalação, suporte, e treinamento para o ambiente de Data Center, conforme especificações, exigências e quantidades estabelecidas neste documento.

Lote	Item	Quantidade	Código Item do SIAD	Descrição do Item
1	1	1	107492	Solução de segurança com funcionalidades de *Firewall*, Sistema de Prevenção de Intrusão (IPS), Redes Virtuais Privadas (VPN), Controle de Aplicações e Ameaças, Filtro de URL e Protocolo de Qualidade de Serviço (*QoS*) Integrados
	2	1	107506	Serviços de atualização e suporte técnico (subscrição) para a solução de *Firewall.*
	3	1	107514	Serviços de instalação, configuração, testes em produção e ajustes dos equipamentos/produtos da solução *Firewall*
	4	1	107590	Serviços de treinamento da solução *Firewall*
2	único	4	1816470	Servidor para Solução *de Segurança*

1.1. ESPECIFICAÇÃO DO OBJETO:

1.1.1. **Lote 1 - Item 1 - Solução de segurança com funcionalidades de *Firewall*, Sistema de Prevenção de Intrusão (IPS), Redes Virtuais Privadas (VPN), Controle de Aplicações e Ameaças, Filtro de URL e Protocolo de Qualidade de Serviço (QoS) Integrados:**

Lote 1 - Item 1 – Solução de Segurança com funcionalidades de *Firewall*, Sistema de Prevenção de Intrusão (IPS), Redes Virtuais Privadas (VPN), Controle de Aplicações e Ameaças, Filtro de URL e Protocolo de Qualidade de Serviço (QoS) Integrados			
Subitem		**Especificação**	**Exigência**
		Solução de segurança com as funcionalidades de *Firewall*, IPS, VPN, Controle de Aplicações, Filtro de URL, *Anti-Malware, Anti-Ransoware,* Anti-	

Descrição	1.0	Virus para controle de ameaças conhecidas e desconhecidas, em alta disponibilidade composta por *software* para *hardware open server*, *software* de gerenciamento, e demais recursos de acordo com as características técnicas e requisitos gerais relacionados neste documento.	Obrigatório
	1.1	A solução deverá ser instalada em ambiente de alta disponibilidade com no mínimo 2 (dois) servidores físicos para o ambiente interno e 2 (dois) servidores físicos para o ambiente externo, fornecidos pela CONTRATANTE, com as características especificadas para item único do lote 2 deste Termo de Referência.	Obrigatório
	1.2	Deverá ser fornecido todo licenciamento de *software* necessário, de forma que a solução a ser fornecida esteja operacional de acordo com as características técnicas e requisitos gerais relacionados neste documento incluindo sistemas operacionais e *hypervisor* de virtualização, caso necessário.	Obrigatório
	1.3	Será aceita atualização do ambiente atual, composto por: • 2 *appliance* em *cluster* externo Check Point 21400; • 2 *appliance* em *cluster* interno Check Point 21400; • Com *Firewall*, IPSec VPN, IPS, *Application Control, Mobile Acess;* • 2 Servidores em *cluster* virtualizados para gerência da solução, licenciado para até 10 *gateways*. De acordo com as características técnicas e requisitos gerais relacionados neste documento.	Opcional
	2.0	NGFW (*Next Generation Firewall*) de no mínimo 16 Gbps (dezesseis gigabits por segundo), independentemente do tamanho do pacote.	Mínimo Obrigatório
	2.1	*Threat Protection* de no mínimo 8 Gbps (oito gigabits por segundo).	Mínimo Obrigatório
	2.2	SSL *Inspection* de no mínimo 6 Gbps	Mínimo

	2.2	(seis gigabits por segundo).	Obrigatório
	2.3	IPsec VPN de no mínimo 14 Gbps (quatorze gigabits por segundo).	Mínimo Obrigatório
Capacidade	2.4	Capacidade para suportar no mínimo u m *throughput* de 8 Gbps (oito gigabits por segundo) de tráfego inspecionado para *Firewall* considerando todas as funcionalidades habilitadas.	Mínimo obrigatório
	2.5	Capacidade de 16 Gbps (dezesseis gigabits por segundo) de NGFW para o perfil recomendado pelo fabricante.	Mínimo obrigatório
	2.6	Permitir 150.000 (cento e cinquenta mil) conexões por segundo (CPS).	Mínimo obrigatório
	2.7	Permitir 10.000.000 (dez milhões) conexões simultâneas.	Mínimo obrigatório
	2.8	Capacidade para suportar *throughput* de 7 Gbps (sete gigabits por segundo) de VPN considerando o algoritmo AES-128.	Mínimo obrigatório
Sistema de Segurança	3.0	Sistema de segurança que provê a capacidade de detecção e bloqueio de ataques sofisticados bem como o reforço granular de políticas de segurança no nível de camada 7 do modelo OSI (aplicação), e atuação como uma plataforma para inspeção do tráfego da rede.	Obrigatório
	3.1	VPN IPSec e SSL, IPS, controle de aplicações, filtragem de conteúdo e gerenciamento da largura de banda integrados (QoS), sem limitação de usuários e ativos, com atualização de todos os componentes (*engines*, assinaturas, etc.) pelo período da garantia.	Obrigatório
	3.2	O sistema deve permitir a aplicação de novas configurações de segurança sem interrupção das operações da rede.	Obrigatório
	3.3	O sistema deve possuir administração unificada da solução, implementada em *hardware* separado e comunicação criptografada entre seus elementos que compõe a solução.	Obrigatório
	3.4	Permitir a configuração de novas funcionalidades (Vazamento de informações (DLP), IPS, VPN, Antivírus, Filtro de Conteúdo, etc.) sem a necessidade de troca do	Obrigatório

		hardware ou reinstalação do *software*.	
	3.5	Todas as funcionalidades de *firewall* deverão ser fornecidas pelo mesmo fabricante de maneira integrada e em uma mesma arquitetura. Devem ainda ter todas as licenças que compõem a solução ativas e válidas de forma perene, mesmo após o término do contrato, exceto para funcionalidades que dependam de atualizações constantes.	Obrigatório
	3.6	O s *logs* e objetos devem estar indexados de forma que permitam a rápida busca das informações usando o padrão *Google-Like.*	Obrigatório
	4.0	A solução deve possibilitar a implementação da tecnologia *Stateful Inspection* que se baseia em análise granular de informações de estado de comunicação e aplicação para conceder o controle de acesso apropriado.	Obrigatório
	4.1	Ter visibilidade das aplicações e aplicar políticas de segurança na camada de aplicação independente de porta ou protocolo.	Obrigatório
	4.2	Deve suportar a criação de regras por geolocalização, tanto na origem, quanto no destino, permitindo que o trafego de determinado País/Países sejam bloqueados ou permitidos.	Obrigatório
	4.3	Deve possibilitar a visualização dos países de origem e destino nos *logs* dos acessos.	Obrigatório
	4.4	A solução de *firewall* deverá suportar o método de identificação e autenticação por usuário.	Obrigatório
	4.5	Capacidade para autenticar sessões para qualquer serviço, isto é qualquer protocolo e/ou aplicação que façam uso dos protocolos TCP/UDP/ICMP.	Obrigatório
	4.6	A solução de *firewall* deverá ser licenciada para usuários e endereços IPs ilimitados.	Obrigatório
	4.7	A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7, oferecendo controle de acesso com suporte a mais de 3.500 (três mil e quinhentas) aplicações, serviços e protocolos pré-definidos.	Obrigatório

Firewall	4.8	Promover a integração com o *Microsoft Active Directory* para a autenticação de usuários, de modo que a solução de *firewall* possa integrar as informações de perfil de usuários armazenadas no serviço de diretórios para realizar a autenticação.	Obrigatório
	4.9	Promover a integração com o protocolo SAML para a autenticação de usuários, pode esse se integrarem com provedor de autenticação em nuvem, como *Azure AD*, *Google Account*, OKTA, de modo que a solução de *firewall* possa integrar as informações de perfil de usuários armazenadas no serviço de diretórios para realizar a autenticação.	Obrigatório
	4.10	Promover a integração com o *Microsoft Active Directory* para identificação transparente de usuários sem necessidade de autenticação direta no *firewall* e implementar políticas de segurança e controle baseadas nestas informações.	Obrigatório
	4.11	Suportar os esquemas de autenticação de usuários tanto para a solução de *firewall* quanto para VPNs como o *tokens* (exemplo *SecureID*), TACACS, RADIUS, senha do sistema operacional, senha do próprio *firewall* e *Microsoft Active Directory*, certificados digitais e dispositivos biométricos.	Obrigatório
	4.12	Deve permitir através de configuração que no momento da aplicação da politica de segurança as sessões tenham que ser reestabelecidas.	Obrigatório
	4.13	Deve permitir através de configuração que no momento da aplicação da politica de segurança as sessões sejam mantidas.	Obrigatório
	4.14	Prover mecanismo contra ataques de falsificação de endereços (IP *Spoofing*) através da especificação da interface de rede pela qual uma comunicação deve se originar.	Obrigatório
	4.15	Suportar controle de aplicações multimídia, tais como voz sobre IP, áudio e vídeo *streaming*.	Obrigatório
	4.16	Capacidade de fazer NAT estático e dinâmico, configurável de forma	Obrigatório

4.16	automática (especificando apenas IP origem e IP traduzido).	Obrigatório
4.17	Capacidade de realizar NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional, possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta.	Obrigatório
4.18	Permitir a inspeção de tráfego HTTPS (*inbound/outbound*).	Obrigatório
4.19	Proteção e suporte às tecnologias de Voz sobre IP SIP e H.323.	Obrigatório
4.20	Suportar H.323 V2, 3 e 4.	Obrigatório
4.21	Suportar H.225 v2, 3 e 4.	Obrigatório
4.22	Suportar H.245 v3, 5 e 7.	Obrigatório
4.23	Suportar NAT para H.323 (tecnologia de Voz sobre IP).	Obrigatório
4.24	Oferecer proteção para seguintes protocolos de VoIP: MGCP e SCCP (*Skinny Client Control Protocol*).	Obrigatório
4.25	Capacidade para suportar IPv6.	Obrigatório
4.26	Capacidade de suportar simultaneamente a criação de regras IPv4 e IPv6.	Obrigatório
4.27	Capacidade de suportar roteamento estático de tráfego Ipv4 e IPv6.	Obrigatório
4.28	Deve suportar a definição de VLAN n o *firewall* conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) *interfaces* o u *subinterfaces* lógicas associadas a VLANs e estabelecer regras de filtragem (*Stateful Firewall*) entre elas. O ID das vlans deve ser de 1 a 4090.	Obrigatório
4.29	Deve possuir suporte a agregação de *links* 802.3ad (LACP).	Obrigatório
4.30	Capacidade de suportar SNMP v2 e v3.	Obrigatório
4.31	Capacidade de integração com MIBs que possam ser compiladas para o sistema de gerenciamento SNMP.	Obrigatório
4.32	Possibilitar o acesso via CLI(Console), SSH, interface Web HTTPS e REST API para configuração e administração local do *Firewall*.	Obrigatório

	4.33	Possibilitar o acesso via REST API, para executar configurações nas p*olicies* de *Firewall* e de controle de ameaças.	Obrigatório
	4.34	Deve permitir a criação de rotas estáticas e suportar, no mínimo, os protocolos de roteamento dinâmico OSPFv2, OSPFv3, BGP e RIP.	Obrigatório
	4.35	Deve possibilitar que as regras de filtragem tenham a capacidade de implementação de CIDR/VLSM.	Obrigatório
	4.36	Possibilitar a atuação como cliente NTP (*Network Time Protocol*).	Obrigatório
	4.37	Deve oferecer as funcionalidades de *backup/restore* e deve permitir ao administrador agendar *backups* da configuração em determinado dia e hora.	Obrigatório
	4.38	O s *b a c k u p s* devem ficar armazenados localmente e deve existir a funcionalidade de transferi-los a um servidor externo via FTP ou SCP.	Obrigatório
	5.0	A solução deve prover a possibilidade de criação de políticas integradas para controle de navegação via navegador e controle de aplicações que utilizem ou não o navegador.	Obrigatório
	5.1	Deve possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.	Obrigatório
	5.2	Deve identificar, permitir ou bloquear aplicações e páginas da Internet, sem a necessidade de liberação/bloqueio de portas e protocolos.	Obrigatório
	5.3	Deve possuir uma base de aplicações incluindo aplicações, "*Widgets*" Web 2.0 e base de URL.	Obrigatório
	5.4	Deve prover a possibilidade de integrar as funções de controle de aplicações e controle de URL's no mesmo equipamento, sem impossibilitar a ativação de outras funcionalidades de segurança, tais como: • IPS; • Antivírus; • Controle de vazamento de informações.	Obrigatório

	5.5	A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser centralizada na mesma gerência.	Obrigatório
	5.6	A solução deve possibilitar a criação de políticas granulares para as funcionalidades de controle de aplicação e filtro.	Obrigatório
	5.7	Deve possibilitar permitir ou bloquear aplicações ou páginas da Internet por: • Aplicação; • URL; • Aplicação e URL; • Categorias; • Nível de risco; • Endereço IP; • Range de IP's; • Usuários; • Grupos de usuários.	Obrigatório
	5.8	Deve possibilitar a integração da solução com base externa do *Microsoft Active Directory* e LDAP, para criação de políticas, possibilitando a criação de regras utilizando: • Usuários; • Grupo de usuários; • Máquinas (estações de trabalho); • Endereço IP; • Endereço de Rede; • Combinação das opções acima.	Obrigatório
	5.9	Deve prover repositório para consulta em tempo real para URL's e aplicações não categorizadas.	Obrigatório
Controle de Aplicações e Filtragem de Conteúdo.	5.10	Deve prover serviço de classificação baseado em "nuvem" (*Cloud based*) para categorização dinâmica do tráfego *Web*.	Obrigatório
	5.11	Deve possibilitar a customização de aplicações, páginas da Internet, categorias e grupos que não estão na base de aplicações e URL, para utilização na criação de políticas.	Obrigatório
		Deve possibilitar a utilização de no mínimo 4 ações nas regras de	

5.12	controle: • Bloquear; • Monitorar; • Informar o usuário; • Interagir com o usuário para decisão da ação (Permitir/Bloquear) possibilitando que o usuário utilize uma justificativa para tal utilização.	Obrigatório
5.13	Deve possibilitar a customização, por regra, da tela de interação com o usuário.	Obrigatório
5.14	Deve permitir diferentes "telas" de interação com o usuário para equipamentos móveis.	Obrigatório
5.15	Deve possibilitar que ações com interações dos usuários sejam aprendidas e utilizadas para eventos similares do mesmo usuário.	Obrigatório
5.16	Deve prover agente na estação do usuário para interação com o usuário quando não for possível via navegador.	Obrigatório
5.17	Deve permitir a configuração na própria regra limite de utilização de banda tanto para tráfego de "*download*" quanto para "*upload*".	Obrigatório
5.18	A solução deve ser capaz de inspecionar o trafego a fim de buscar aplicações que possam comprometer a segurança da CONTRATANTE, como P2P (KaZaa, Gnutella, Morpheus, BitTorrent, µTorrent) e Ims (Yahoo!, MSN/Skype, ICQ), mesmo quando elas pareçam ser tráfego válido.	Obrigatório
5.19	Deve oferecer proteção contra *MSN Messenger* / Skype via MSNMS e SIP.	Obrigatório
5.20	O administrador deve ser capaz de funcionalidades específicas de páginas Web 2.0 ou aplicações. Por exemplo: bloquear o *c h a t* e a visualização de vídeos no *Facebook*; bloquear somente a transferência de arquivos no MSN, etc.	Obrigatório
5.21	O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos.	Obrigatório

	5.22	O administrador deve ser capaz de configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.	Obrigatório
	5.23	Deve oferecer a opção de bloquear controles *ActiveX* e *applets* Java que possam comprometer usuários *web.*	Obrigatório
	5.24	A solução deve permitir a inspeção de tráfego sobre o protocolo HTTPS (*Inbound/outbound*).	Obrigatório
	6.0	A solução de Segurança deve ter uma solução de VPN integrada (compartilhar o mesmo *hardware*) para que se possa adicionar e suportar o ambiente de VPN.	Obrigatório
	6.1	O *software* de VPN e *firewall* devem compartilhar o mesmo *hardware* e sistema operacional, e também os recursos de *cluster*.	Obrigatório
	6.2	A funcionalidade de IPSec / VPN de todo o *hardware* ofertado deve ser a mesma e deve ser licenciada para funcionamento em *cluster* ativo-ativo e *cluster* ativo-passivo.	Obrigatório
	6.3	Deve permitir habilitar e desabilitar túneis de VPN a partir da interface gráfica da solução, facilitando o processo de *throubleshooting*.	Obrigatório
	6.4	Deve ser fornecida licenciamento para criação de no mínimo 8.000 (oito mil) VPN do tipo *site-to-site*.	Obrigatório
	6.5	Deve suportar o conceito de "comunidades de VPN" (comunidade de *gateways* VPN que se comunicam através de túneis criptografados) permitindo uma configuração centralizada e simplificada dos vários dispositivos de VPN (*gateways*) participantes de tal comunidade, evitando que a configuração seja feita em cada um destes dispositivos por vez.	Obrigatório
	6.6	Deve suportar esquemas de VPN *site-to-site* em topologias "*Full Meshed*" (cada *gateway* tem um *link* específico para os demais *gateways*), "*Star*" (*gateways* satélites se comunicam somente com o *gateway* central), "*Hub and Spoke*" (onde o *gateway* definido como Hub tem por responsabilidade redirecionar o tráfego para o seu *gateway* destino (*spoke*).	Obrigatório

6.7	Deve incluir suporte a *client-to-site* baseado em IPSEC. (mínimo 5.000 usuários simultâneos).	Mínimo Obrigatório
6.8	Permitir suporte integrado à VPN SSL client-to-site nativo ou via licenciamento adequado incluso. (mínimo 2.500 usuários simultâneos através de browser).	Mínimo Obrigatório
6.9	Suportar os seguintes algoritmos de criptografia simétricos: AES256, AES128, DES, 3DES para fases I e II, assegurando que somente os *peers* que fazem parte da VPN tenham capacidade de entender a mensagem final.	Obrigatório
6.10	Permitir que os *gateways* VPN (em uma topologia *site-to-site*) se autentiquem via *preshared secret* e/ou certificados digitais.	Obrigatório
6.11	Suportar *Main Mode e Aggressive mode* em IKE *Phase* I.	Obrigatório
6.12	Deve suportar integridade de dados MD5 e SHA1.	Obrigatório
6.13	Suportar conexões VPN *Client to Site* a partir de aplicativos disponíveis no Microsoft Market.	Obrigatório
6.14	Suportar conexões VPN advindas de *clients* L2TP/IPSec nativos em plataformas *Windows* 7, 8, 10 e *Windows Server* 2008 e superiores.	Mínimo Obrigatório
6.15	Suportar os algoritmos para geração de chave publica: RSA e *DiffieHellman*, abrangendo os seguintes *groups*: *Group* 1 (768 bits), *Group* 2 (1024 bits), *Group* 5 (1536 bits) e *Group* 14 (2048 bits).	Obrigatório
6.16	Suporte para que os clientes VPN possam ter, opcionalmente, camada de *firewall* pessoal (usando o mesmo *software*) para proteção da estação com mecanismos de verificação de configurações desta estação (ex. AntiVirus ativo e atualizado), tendo uma política administrada de forma centralizada pela mesma console de VPN.	Obrigatório
6.17	Caso necessite de agentes VPN, o cliente IPSEC VPN incluso deve suportar *roaming* (mudança de redes/interfaces e mudança de endereço IP sem perda da conexão	Obrigatório

VPN	6.17	VPN) e *Auto-Connect* (uma conexão é feita automaticamente quando o *endpoint* está fora da rede corporativa e uma aplicação necessita acesso a essa rede).	Obrigatório
	6.18	Suportar os seguintes esquemas de autenticação de usuários por VPN: usuário e senha em base do próprio sistema de *Firewall*, Serviço de Diretório *Microsoft Active Directory*, certificação digital por meio de certificados emitidos por Autoridade Certificadora no padrão ICP-Brasil.	Obrigatório
	6.19	Capacidade de otimizar o rendimento de VPN através de técnicas de aceleração por *software*.	Obrigatório
	6.20	Suportar autoridade certificadora integrada ao *gateway* VPN Autoridade Certificadora integrada à VPN ou a sua console de administrativa como parte nativa da solução, de maneira que se emitam certificados digitais para usuários de VPN e/ou *gateways* de VPN com os quais se estabeleçam comunicação e/ou os componentes da solução (tais como *console* de administração, administradores, módulos, etc.).	Obrigatório
	6.21	Fácil integração com certificados digitais (PKI) de terceiros, que cumpram com o padrão X.509 para não repúdio de transações por VPN. Pelo menos oferecer a capacidade de integração com 4 diferentes autoridades certificadoras integráveis.	Obrigatório
	6.22	Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados nos formatos: PKCS#12, CAPI e *Entrust* utilizados no processo de autenticação entre um *gateway* VPN e um usuário remoto (*client-to-site* VPN).	Obrigatório
	6.23	Suportar a solicitação de emissão de certificados a uma CA *trusted (enrollment*) via SCEP.	Obrigatório
	6.24	Suporte a algoritmos de compressão de dados, tanto para as VPNs *site-to-site* como para as VPNs *client-to-site*, realizadas com os clientes próprios.	Obrigatório
	6.25	Oferecer proteção contra ataque IKE DoS, fazendo a distinção entre *peers* conhecidos e desconhecidos.	Obrigatório

	6.26	Suportar NATT (NAT *Traversal Tunneling*).	Obrigatório
	6.27	Suportar VPN baseada em rotas, de maneira a conhecer a rota seguinte para envio do tráfego da VPN. Deve suportar ao menos rotas estáticas com opção para suporte à BGP e OSPF como protocolos de roteamento dinâmico para essa característica.	Obrigatório
	6.28	Clientes IPSec do mesmo fabricante devem estar disponíveis para pelo menos as seguintes plataformas: *GNU/Linux*, *Windows* 7,8, 10 (32bits e 64bits)**,** *Iphone/Ipad* e *Android*.	Mínimo Obrigatório
	6.29	O acesso VPN SSL deve ser possível para pelo menos as seguintes plataformas: *GNU/Linux*, *Windows* 7,8, 10 (32bits e 64bits)**,** *Iphone/Ipad* e *Android*.	Mínimo Obrigatório
	6.30	Deve incluir gerenciamento centralizado de VPNs, com a possibilidade de criar várias VPNs ao mesmo tempo.	Obrigatório
	6.31	Deve permitir que o administrador aplique regras de segurança para controlar o tráfego dentro da VPN	Obrigatório
	6.32	Deve incluir a funcionalidade para estabelecer VPNs com *gateways* com IPs públicos dinâmicos.	Obrigatório
	6.33	Deve possuir Portal SSL para acesso às aplicações internas.	Obrigatório
	6.34	Deve prover acesso via VPN SSL utilizando navegador (*Browser*) sem a necessidade de um cliente instalado na estação. Compatível com os sistemas operacionais Linux, Windows e MacOS.	Obrigatório
	6.35	Para o acesso via VPN SSL, a solução deverá alocar um endereço IP para estação remota para evitar problemas de roteamento.	Obrigatório
	7.0	As funcionalidades de IPS e *firewall* devem ser implementadas em um mesmo chassi, sendo que a comunicação entre eles deverá ser interna, sem a necessidade de uso de quaisquer interfaces externas.	Obrigatório
		Deve incluir pelo menos os seguintes mecanismos de detecção:	

7.1	• Assinaturas de vulnerabilidades e *exploits*; • Assinaturas de ataque; • Validação de protocolo; • Detecção de anomalia; • Detecção baseada em comportamento; • Nível de confiança de detecção de ataque.	Obrigatório
7.2	O administrador deve ser capaz de configurar a inspeção somente para tráfego entrante (*inbound*).	Obrigatório
7.3	O IPS deve incluir pelo menos 10.000 (dez mil) definições de ataques que protejam tanto clientes/servidores.	Mínimo Obrigatório
7.4	O IPS deve oferecer ao menos duas políticas pré-definidas que podem ser usadas imediatamente.	Mínimo Obrigatório
7.5	As regras de IPS podem ser associadas a um escopo especifico, em que um conjunto especifico de assinaturas estão associadas a um conjunto especifico de objetos de rede.	Obrigatório
7.6	O IPS deve incluir a habilidade de interromper temporariamente as proteções para fins de *troubleshooting.*	Obrigatório
7.7	A solução também deve permitir configuração de "*fail-open*" lógico, da função de IPS, em situações que coloquem em risco o funcionamento do *Firewall.*	Obrigatório
7.8	O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento.	Obrigatório
7.9	O administrador deve ser capaz de ativar novas proteções baseado em parâmetros configuráveis (impacto no desempenho, severidade da ameaça, proteção dos clientes, proteção dos servidores).	Obrigatório
7.10	O administrador deve ser capaz de ativar novas proteções baseado em ataques associados a um determinado VENDOR (*Microsoft, Oracle, Siemens*, *etc.*).	Obrigatório

	7.11	O administrador deve ser capaz de ativar novas proteções baseadas em ataques associados a ataques mais comuns.	Obrigatório
	7.12	O administrador deve ser capaz de ativar novas proteções baseadas no score do CVE.	Obrigatório
	7.13	O administrador deve ser capaz de desativar proteções baseadas em ataques obsoletos.	Obrigatório
	7.14	A solução deve ser capaz de detectar e prevenir as seguintes ameaças: *Exploits* e vulnerabilidades específicas de clientes e servidores, mal uso de protocolos, comunicação *outbound* d e *malware*, tentativas de *tunneling*, controle de aplicações, ataques genéricos sem assinaturas pré-definidas.	Obrigatório
	7.15	Deve oferecer proteções de seguir o uso de aplicações específicas como *peer-to-peer*, com a opção de bloquear estas aplicações.	Obrigatório
	7.16	Para cada proteção, a descrição da vulnerabilidade e da ameaça, severidade da ameaça e nível de confiança de detecção de ataque devem estar inclusos.	Obrigatório
	7.17	Para cada escopo de proteção pode se adicionar exceções baseadas em FQDN e País.	Obrigatório
	7.18	Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na fonte, destino, serviço ou qualquer combinação dos três.	Obrigatório
	7.19	A solução deve fazer captura de pacotes para proteções específicas.	Obrigatório
	7.20	A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, redes e VoIP.	Obrigatório
Controle de Ameaças	7.21	Deve incluir a habilidade de detectar e bloquear ataques conhecidos e desconhecidos, protegendo de, pelo menos, os seguintes ataques conhecidos: IP *Spoofing*, SYN *Flooding*, *Ping of death*, ICMP *Flooding*, *Port Scanning*, ataques de força bruta a IKE e *man-in-the-middle*	Obrigatório

	com VPNs.	
7.22	Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades em diversas áreas de interesse do administrador e a evolução no tempo. As diferentes áreas de interesse devem ser definidas usando filtros customizáveis para selecionar alertas baseados em qualquer propriedade ou combinação de propriedades do mesmo, incluindo pelo menos: origem, destino, serviço, tipo e nome do alerta.	Obrigatório
7.23	A solução deve permitir a configuração de inspeção do IPS baseado em políticas que utilizem o posicionamento geográfico de origens e destinos do tráfego.	Obrigatório
7.24	A solução deve permitir a inspeção de tráfego sobre o protocolo HTTPS (*Inbound/outbound*).	Obrigatório
7.25	A solução deve permitir a pré-configuração de no mínimo 10 perfis de proteção de IPS que podem ser utilizados a qualquer momento.	Obrigatório
7.26	O sensor do sistema deve impedir *network malware*, incluindo: *Worms* e Virus, *Ransomware*, *Backdoors* e *Trojans*, *Cross-Site Scripting*, SQL *Injections*, *Spyware*, *Phishing*, *Rootkits*, *Anonymizers*, IRC *Bots communications.*	Obrigatório
7.27	O sensor do sistema deve impedir comunicação com C&C(*command-and-control*).	Obrigatório
7.28	Protocolos de Rede e Serviços de Proteção (RPC, NetBIOS, Telnet, etc).	Obrigatório
7.29	O sensor do sistema deve ser capaz de detectar e prevenir ataques baseados em protocolos como *malformed* ICMP *packets* (*Ping of Death*) , *source routed pings* (*Land attacks*), etc.	Obrigatório
7.30	O sensor do sistema não deve gerar alertas sobre *replays* de ataques *stateless* de assinaturas de ataques válidos que geram grande volumes de *trigges* de falsos ataques capazes de ofuscar o conteúdo do ataque válido.	Obrigatório
	O sensor do sistema deve ser capaz	

	7.31	de remontar um pacote IP de um ataque de pacote fragmentado antes da aplicação da regra do IPS.	Obrigatório
	7.32	O sensor do sistema deve ser capaz de realizar inspeção e remontagem de fluxo para evitar técnicas de segmentação TCP, tais como: *interleaved duplicate segments invalid* TCP c*hecksums, segment overlap*, etc.	Obrigatório
	7.33	O sensor do sistema deve bloquear a atividade da propagação de *malwares* sem bloquear aplicações legítimas, mesmo quando eles são executados no mesmo computador.	Obrigatório
	7.34	Deve ser possível a implementação em tempo real de bloqueio de trafego suspeito sem a necessidade de mudanças nas regras de acesso.	Obrigatório
	7.35	Novas assinaturas de IPS podem ser automaticamente instaladas nos gateways assim que disponibilizadas pelo fabricante.	Obrigatório
	7.36	A solução deve ser capaz de reconstruir arquivos do padrão office (.doc, .xlxs) e PDF em busca de ameaças não conhecidas, paciente de dia zero.	Obrigatório
	7.37	A solução deve ser capaz de reconstruir arquivos do padrão office (.doc, .xlxs) e entregar ao usuário um cópia em PDF.	Mínino obrigatório
	7.38	A solução deve ser capaz de realizar emulação de arquivos em busca de anomalias ao acesso da CPU em busca de ameaças não conhecidas.	Obrigatório
	7.39	A solução deve ser capaz de realizar emulação de arquivos antes que os mesmos sejam entregues ao usuário.	Obrigatório
	7.40	A solução deve realizar a emulação de arquivos em *Cloud*.	Obrigatório
	7.41	A solução deve permitir a inspeção de tráfego sobre o protocolo HTTPS (*Inbound/outbound*).	Obrigatório
	7.42	A solução deve permitir a utilização de no mínimo 4 perfis de proteção contra ameaças preconfiguradas, que permitam a solução adotar as melhores práticas de segurança sem intervenção humana.	Obrigatório

QoS	8.0	A solução de Segurança deve ter uma solução de *QoS* integrada (compartilhar o mesmo *hardware*) para que se possa adicionar suporte a *QoS*.	Obrigatório
	8.1	Suportar tecnologia de *QoS* baseada em cotas inteligentes para segurança e produtividade.	Obrigatório
	8.2	Oferecer suporte a *QoS* para tráfego criptografado.	Obrigatório
	8.3	Suporte a monitoramento gráfico do tráfego que está passando pelo dispositivo em tempo real.	Obrigatório
	8.4	Capacidade de administração da largura de banda por IP origem, IP destino, direção (de dentro para fora ou de fora para dentro) pelo usuário e horário.	Obrigatório
	8.5	Capacidade de administração da largura de banda por usuário ou grupo de usuários.	Obrigatório
	8.6	Suporte a limites (largura de banda máxima a ser utilizada), garantias (mínimo reservado) e pesos relativos (prioridades) como ações para o tráfego classificado.	Obrigatório
	8.7	Suporte integrado, como parte nativa da solução, a serviços diferenciados (*DiffServ*).	Obrigatório
	8.8	Permitir que o tráfego marcado (*DiffServ Code Point– DCP*) seja entendido e priorizado inclusive em estruturas de redes MPLS provendo QoS de ponta a ponta.	Obrigatório
	8.9	Suporte a controles com filas de baixa latência (*Low Latency Queues – LLQ*) para acelerar o tráfego sensível a atraso.	Obrigatório
	8.10	Suporte à alta disponibilidade transparente, ou seja, sem perda de conexões em texto claro, criptografadas ou classificadas pelo *QoS*, em caso de falha de um dos nós.	Obrigatório
	8.11	Suporte a balanceamento de carga entre os gateways de *Firewall/VPN/QoS*.	Obrigatório
	8.12	Capacidade integrada de *QoS* tanto para tráfego em texto claro como para tráfego *VPN*.	Obrigatório

Tolerância a Falhas	9.0	A solução fornecida deverá ser capaz de suportar a criação de *clusters* com tolerância a falhas, nos modos Alta-Disponibilidade (HA) e/ou cooperativo, em modo ativo-ativo com balanceamento interno.	Obrigatório
	9.1	A solução deve ser capaz de suportar *cluster* em modo ativo-ativo com no mínimo 2 (dois) membros.	Obrigatório
	9.2	No modo Alta-Disponibilidade, a configuração seria a mesma do modo *failover*, porém toda a configuração de estado seria replicada. Desta forma, conexões ativas continuariam funcionando através do *firewall* secundário.	Obrigatório
	9.3	No modo cooperativo, pelo menos 2 *firewalls* deverão estar em funcionamento simultaneamente, dividindo o tráfego de rede entre eles de forma automática e replicando configuração e estado das conexões também de forma automática.	Obrigatório
	9.4	No modo cooperativo e alta-disponibilidade, descritos no item anterior, no caso de queda de um dos *firewalls*, não poderá haver perdas das conexões ativas através do *cluster*, mesmo que estas passem por NAT ou VPN.	Obrigatório
	9.5	Poderão ser aceitos equipamentos adicionais para complementar as funcionalidades de *cluster* exigidas nesta especificação, contando que os itens de desempenho, quantidade de portas e alta disponibilidade sejam cumpridas para cada conjunto de equipamentos e que os equipamentos sejam homologados pelo fabricante do *software* de *firewall.*	Obrigatório
	10.0	A solução de gerência centralizada das Políticas de Segurança dos *firewalls* deve ser implementada em *hardware* separado.	Obrigatório
	10.1	A solução de gerência das Políticas deve replicar as alterações para todos os *gateways* envolvidos.	Obrigatório
	10.2	A especificação do *hardware* necessário para gerência, *logs* e monitoração deve ser fornecida pelo fornecedor, seguindo padrões do fabricante da solução.	Obrigatório

10.3	Deverá ser possível a instalação do *software* de gerência em ambiente virtualizado *Vmware*, *MS Hyper-V* e KVM.	Obrigatório
10.4	Deve disponibilizar acesso por meio de *browser* ou *client* do próprio fabricante para visualização de políticas, objetos e usuários a fim de prover acesso para gerentes e auditores sem a necessidade de utilizar a console completa.	Obrigatório
10.5	O sistema deve prover habilidade de criar regras/politicas de *IPS* para cada interface, virtual interface ou zona de segurança definida.	Obrigatório
10.6	O sistema de gerencia deve possibilitar o *upgrade* dos *gateways* de segurança através de interface especifica para isso.	Obrigatório
10.7	O sistema deve suportar upgrade de *software/ruleset* que permitam ao usuário atualizar o *IPS* sem perda de conectividade de rede.	Obrigatório
10.8	Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de *firewall*, gerência, armazenamento de logs e emissão de relatórios.	Obrigatório
10.10	Deve oferecer opção de autorizar e bloquear os acessos dos usuários à visualização pelo *browser* ou *client* do próprio fabricante.	Obrigatório
10.11	O acesso por meio *browser* deve ocorrer sobre SSL.	Obrigatório
10.12	Deve permitir a criação de regras por intervalo de tempo e/ou período(data e horário de início e fim de validade).	Obrigatório
10.13	Deve prover, em cada regra, a informação da utilização da mesma. No mínimo: • Percentual de utilização em relação a outras regras; • Número de vezes em que a regra foi utilizada.	Obrigatório
10.14	Deve suportar que diferentes usuários utilizem a mesma politica no modo de edição ao mesmo tempo.	Obrigatório

10.15	Deve suportar que o usuário tenha mais de sessão para edição simultaneamente.	Obrigatório
10.16	Deve permitir a segregação de atividades, em que um usuário possa alterar apenas as funções (por exemplo Controle de Aplicação), mas não possa alterar as configurações de *IPS*.	Obrigatório
10.17	Deve suportar diferentes perfis de administração, disponibilizando, pelo menos, os seguintes: *read/write, read only*, gerenciamento de usuários e visualização de *logs*.	Obrigatório
10.18	Deve incluir CA interna x.509 capaz de gerenciar certificados para *gateways* e usuários permitindo autenticação em *VPNs*.	Obrigatório
10.19	Deve incluir a capacidade de confiar em CAs externas ilimitadas com a opção de verificar o certificado de cada *gateway* externo através de, no mínimo, DN(*Distinguished Name*) e IP.	Obrigatório
10.20	Deve permitir a criação de diversos perfis de IPS a serem aplicados a diferentes *gateways*.	Obrigatório
10.21	Deve permitir incorporar automaticamente novas proteções de IPS baseadas, no mínimo, em severidade e nível de confiança da proteção.	Obrigatório
10.22	Deve possuir a facilidade de busca com, no mínimo, as opções de consulta: quais objetos contêm IPs específicos ou parte deles, busca por objetos duplicados, busca por objetos não utilizados e listar em quais regras um objeto é utilizado.	Obrigatório
10.23	Deve possuir a opção de segmentar as regras de segurança através de rótulos com a finalidade de organizar as políticas.	Obrigatório
10.24	Deve prover a opção de salvar automaticamente e manualmente versões de políticas.	Obrigatório
10.25	Deve prover a funcionalidade de mover objetos e serviços entre as regras e de uma lista de objetos e serviços para uma regra.	Obrigatório
10.26	A solução deverá gerenciar de forma centralizada as licenças dos *gateways*	Obrigatório

		controlados por ela.	
	10.27	Deve prover a funcionalidade de provisionamento de licenças a partir de um pool de licenças disponível.	Obrigatório
	10.28	As funcionalidades da solução de armazenamento de logs deverão prover as seguintes características: Deverá possibilitar a filtragem de eventos baseado em diversas categorias (IP origem, porta origem, IP destino, porta destino, interface, categoria de ataque, *translated* IP, *translated port*, entre outras) simultaneamente; Deverá possibilitar a filtragem de eventos relacionados a ação do administrador. No mínimo: • "*login*" e "*logout*"; • Alteração de política; • Aplicação de alteração de política.	Obrigatório
	10.29	As buscas aos *l o g s* devem ser *google-like*	Obrigatório
	10.30	Deverá possibilitar integração com soluções de mercado focadas em correlação de eventos.	Obrigatório
	10.31	Deverá possibilitar a visualização dos eventos das soluções de segurança na própria solução de gerência.	Obrigatório
	10.32	Deve incluir um mecanismo automático de captura de pacotes para eventos de IPS com a finalidade facilitar análise forense.	Obrigatório
	10.33	A solução deverá diferenciar os *logs* para atividades comuns de usuário e *logs* relacionados à gerencia de políticas de segurança.	Obrigatório
	10.34	A solução deverá permitir configurar para cada tipo de regra ou evento pelo menos três das opções: *log*, alerta, enviar *trap* SNMP, envio de e-mail, execução de *script* definido pelo usuário.	Obrigatório
	10.35	A solução deverá incluir a opção de alterar uma regra ativa a partir da interface gráfica de visualização de *logs*.	Obrigatório
Gerência Centralizada	10.36	A solução deve ser capaz de exportar os *logs* para uma base de dados ou	Obrigatório

do Sistema de Segurança		repositório externo.	
	10.37	A solução deve suportar a troca automática de arquivo de *log*, regularmente ou através do tamanho do arquivo.	Obrigatório
	10.38	Deve permitir a visualização simultânea de utilização dos recursos do *gateway*. No mínimo: • Utilização de CPU; • Utilização de Memória; • Utilização de disco; • Quantidade de conexões simultâneas; • Quantidade de novas conexões por segundo; • Pacotes bloqueados; • Situação (status) geral das funções de *firewall;* • Situação (status) das funcionalidades de segurança ativas no *firewall.*	Obrigatório
	10.39	Deve permitir a criação de filtros com base em pelo menos as seguintes características do evento: endereço IP de origem e destino, serviço, tipo de evento, severidade do evento e nome do ataque.	Obrigatório
	10.40	Deve permitir ao administrador o agrupamento de eventos baseado em qualquer uma das opções de filtragem, incluindo vários níveis de alinhamento.	Obrigatório
	10.41	Prover mecanismo de visualização de eventos das soluções de segurança, com uma prévia sumarização para fácil visualização de no mínimo as seguintes informações: • Funções de segurança mais utilizadas; • Origem mais utilizada; • Destino mais utilizado; • Regras mais utilizadas; • Usuários com maior atividade.	Obrigatório
	10.42	Deve prover funcionalidades para análise avançada. No mínimo: • Visualizar quantidade de tráfego utilizado de aplicações e navegação;	Obrigatório

	• Gráficos; • Estatísticas.	
10.43	O administrador deve ser capaz de atribuir filtros para acompanhamento em tempo real, mostrando todos os eventos que corresponda a esse filtro. Permitindo ao operador a concentrar-se sobre os eventos mais importantes.	Obrigatório
10.44	Deve detectar ataques de negação de serviço e correlacionar eventos de todas as fontes.	Obrigatório
10.45	Deve suportar a detecção de ataques de força bruta para quebra de credencial.	Obrigatório
10.46	Deve permitir a geração de relatórios com horários predefinidos, diários, semanais e mensais. Incluindo principais eventos, principais origens, principais destinos, principais Serviços, principais origens e os seus principais eventos, principais destinos e seus principais eventos e principais serviços e seus principais eventos.	Obrigatório
10.47	Possibilitar o envio de eventos para Sistema de Gerenciamento de Informações de Eventos (SIEM), utilizado pela SEF-MG, HP Arcsight.	Obrigatório
10.48	Os *logs* podem ser enviados para servidores externos utilizando-se de criptografia TLS.	Obrigatório
10.49	Possibilitar reação automática para determinados tipos de eventos.	Obrigatório
10.50	Na função de reação automática deve ser permitida a criação de "*script*".	Obrigatório
10.51	Deve possibilitar a visualização geográfica dos eventos de segurança.	Obrigatório
10.52	A ferramenta de relatórios deve fornecer relatórios consolidados e predefinidos sobre: • O volume de conexões que foram bloqueadas pela solução; • Principais fontes de conexões bloqueadas, seus destinos e serviços; • Principais regras usadas pela solução; • Principais ataques detectados	Obrigatório

	pela solução e indicação das suas principais fontes e destinos; • Número de políticas instaladas e desinstaladas na solução; • Principais serviços de rede; • Indicação dos serviços que mais utilizaram tráfego criptografado; • Principais usuários VPN.	
10.53	A ferramenta de relatórios deve suportar pelo menos os seguintes filtros: endereço de origem, endereço de destino, usuário, nome do ataque e número da regra.	Obrigatório
10.54	A ferramenta de relatórios deve permitir a personalização de relatórios pré-definidos.	Obrigatório
10.55	Deve suportar, no mínimo, dois dos seguintes formatos de relatórios: MHT, HTML, PDF, *Microsoft Excel*, *Microsoft Visio*, ODF e CSV.	Obrigatório
10.56	Deve suportar a distribuição automática de relatórios por e-mail.	Obrigatório
10.57	Deve permitir a integração com nuvens públicas: *Azure, AWS, GCP, Oracle Cloud, Alibaba*.	Obrigatório
10.58	Deve permitir a integração com nuvens privadas: *VMWare NSX, Cisco ACI, Openstack e Nuange.*	Obrigatório
10.59	A integração com nuvens públicas e privadas deve permitir que uma máquina criada em um desses ambiente receba automaticamente permissão de acesso sem a necessidade de se aplicar uma nova política.	Obrigatório
10.60	Deve possuir mecanismo *workflow* para autorização de mudança com perfil de operador, aprovador e gestor.	Obrigatório
10.61	Deve possuir ferramenta de verificação de *compliance* para as seguintes regulamentações: SOX, NIST, GDPR, ISO 27001, ISO 27002.	Obrigatório
10.62	A atualização da solução de todos os elementos da solução deve ser realizada através da console de gerenciamento.	Obrigatório
	A gerência deve permitir	

	10.63	versionamento das mudanças realizadas no ambiente.	Obrigatório
	10.64	A gerência deve permitir retornar o ambiente para uma versão anterior.	Obrigatório
	10.65	Possibilitar o acesso via CLI (*Console*), SSH, interface Web HTTPS e REST API para configuração e administração local do *Firewall*.	Obrigatório
	10.66	Possibilitar o acesso via REST API, para executar configurações nas Políticas de *Firewall* e de Controle de Ameaças.	Obrigatório

1.1.2. **Lote 1 - Item 2 - Serviços de atualização e suporte técnico (subscrição) para a solução de *Firewall:***

Lote 1 - Item 2 – Serviços de atualização e suporte técnico (subscrição) para a solução de *Firewall.*			**Quantidade: 1 unidade**
Subitem		**Especificação**	**Exigência**
	1.0	A solução de segurança (Lote1 - item 1) deve possuir garantia de 12 (doze) meses com um período de disponibilidade para chamada de manutenção de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.	Obrigatório
	1.1	Os produtos fornecidos no Lote1 - item 1 deverão ter garantia original de fábrica na totalidade de seu funcionamento pelo período mínimo de 12 (doze) meses, contados a partir da data de expedição do Termo de Recebimento Definitivo pela SEF/MG.	Obrigatório
	1.2	Os chamados de manutenção, dúvidas, entre outros itens abaixo citados, ou até mesmo para contato com o fabricante, serão aberto diretamente pela CONTRATADA para que essa possa intermediar a manutenção, duvidas, entre outros itens abaixo citados. Não deve haver limite para aberturas de chamados, sejam de: • Solução de problemas de configuração e utilização da solução fornecida, inclusive virtualização; • Esclarecimentos de dúvidas sobre a configuração e a utilização dos equipamentos/produtos;	Obrigatório

		• Implementação e customização de novas funcionalidades nos componentes da solução; • Instalação de atualizações de *software* dos produtos fornecidos; • Resolução de problemas na solução ofertada.	
	1.3	A abertura de chamados poderá ser realizada através de telefone 0800 do fabricante ou parceiro/fornecedor, ou através da página da WEB do fabricante ou parceiro/fornecedor ou através de endereço de e-mail do fabricante ou parceiro/fornecedor.	Obrigatório
	1.4	A abertura de chamados através de telefone 0800 deverá ser realizada inicialmente em português.	Obrigatório
Suporte, Garantia e Atualização	1.5	A CONTRATADA deverá realizar os atendimentos, observando a classificação dos problemas reportados e prazo de conclusão do chamado a contar da abertura do chamado técnico de acordo com seu grau de severidade, segundo a seguinte classificação: • **Severidade 1**: problemas que tornem qualquer um dos nós da solução inoperante. **Prazo: 2 (duas) horas,** com atendimento *in-loco*. • **Severidade 2:** problemas ou dúvidas que prejudicam a operação da infraestrutura de rede, mas que não interrompem o acesso aos dados. **Prazo: 8 (oito) horas** com atendimento *in-loco* ou remoto, a critério da CONTRATADA; • **Severidade 3**: problemas ou dúvidas que criam algumas restrições à operação da infraestrutura. **Prazo: 24 (quarenta e oito) horas** com atendimento *in-loco* ou remoto, a critério da CONTRATADA; • **Severidade 4**: problemas ou dúvidas que não afetam a operação da infraestrutura. **Prazo: 3 (três) dias úteis** com atendimento *in-loco* ou remoto, a critério da CONTRATADA. Entende-se por término do atendimento aos chamados de	Obrigatório

	suporte técnico a disponibilidade do equipamento para uso em perfeitas condições de funcionamento no local onde está instalado.	
1.6	Conforme a gravidade ou criticidade do problema a ser resolvido, a CONTRATADA deverá viabilizar o escalonamento do incidente para a área de suporte ou engenharia do fabricante dos produtos devidamente capacitada a resolver o problema, sem custo adicional para a CONTRATANTE.	Obrigatório
1.7	A CONTRATADA deverá responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores do quadro da empresa, assim como pelos efeitos delas advindos na execução das atividades previstas nesta especificação técnica ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por estes executadas.	Obrigatório
1.8	A CONTRATADA deverá fornecer e aplicar os *patches* de correção, em data e horário a serem definidos pela CONTRATANTE, sempre que forem encontradas falhas de laboratório (*bugs*) ou falhas comprovadas de segurança nos equipamentos/produtos, objeto deste Termo de Referência.	Obrigatório
1.9	O serviço de suporte técnico permite o acesso da CONTRATANTE à base de dados de conhecimento do fabricante dos equipamentos/produtos, provendo informações, assistência e orientação para: • Instalação, desinstalação, configuração e atualização de imagem de *software*; • Aplicação de correções (*patches*) de *software*; • Diagnósticos, avaliações e resolução de problemas; características dos equipamentos/produtos e demais atividades relacionadas à correta operação e funcionamento dos mesmos.	Obrigatório
	O s *patches* e novas versões de *software* integrante da solução ofertada deverão ser instalados pela CONTRATADA, após aprovação da	

	1.10	CONTRATANTE, tão logo estas se tornem disponíveis. A cada atualização realizada deverão ser fornecidos os manuais técnicos originais e documentos comprobatórios do licenciamento da nova versão/*patch.*	Obrigatório
	1.11	Deverá ser garantido à CONTRATANTE o pleno acesso ao site do fabricante dos equipamentos e *software*. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e *software* especificados, além de permitir *downloads* de quaisquer atualizações de *software* ou documentação deste produto, inclusive base de reputação (subscrição) de todos os itens necessário para total funcionamento da solução.	Obrigatório
	1.12	Durante o período de suporte técnico, devem ser disponibilizados e instalados, sem ônus à CONTRATANTE, todas as atualizações de *software.*	Obrigatório

1.1.3. **Lote 1 - Item 3 - Serviços de instalação, configuração, testes em produção, ajustes dos equipamentos/produtos, e repasse de conhecimento da solução - Firewall:**

Lote 1 - Item 3 – Serviços de instalação, configuração, testes em produção, ajustes dos equipamentos/produtos, e repasse de conhecimento da solução - Firewall			**Quantidade: 1 unidade**
Subitem		**Especificação**	**Exigência**
	1.0	A configuração da solução será realizada na área de Tecnologia da Informação da CONTRATANTE, em Belo Horizonte - MG pela CONTRATADA.	Obrigatório
	1.1	Para a execução dos serviços de instalação, configuração, testes em produção e ajustes, a CONTRATADA deverá alocar profissionais devidamente certificado pelo fabricante, para as tecnologias envolvidas ou, o profissional do próprio fabricante da solução, tendo em vista a criticidade do ambiente.	Obrigatório
		A CONTRATADA deverá entregar à CONTRATANTE, em até (15) dias úteis, após assinatura do contrato,	

	1.2	uma proposta de projeto / migração para a implementação da solução de Segurança descrita no item 1 – Lote 1. Deverá ser entregue em mídia digital no formato *Portable Document File* (PDF), contendo um rascunho do projeto da arquitetura e topologia, com as informações necessárias, abrangendo todo o *hardware* e *software* envolvidos. Deverá ainda ser apresentado um Plano de Implantação da Solução, contendo, no mínimo, os seguintes itens: • Atividades a serem desempenhadas; • Roteiro de implantação; • Cronograma previsto para intervenção no ambiente da CONTRATANTE (a se acordar com a CONTRATANTE); • Responsáveis envolvidos nas fases de implantação e testes; • Plano de retorno (*rollback*) em caso de falha na implantação.	Obrigatório
	1.3	A CONTRATADA deverá disponibilizar 1 (um) gerente de projeto responsável por acompanhar a instalação e configuração dos equipamentos. Este profissional deverá no minimo: • Fazer uma reunião de alinhamento e *overview* do escopo do projeto, gerenciamento de expectativas, planos de comunicação e requisitos necessários para implementação; • Realizar a coleta de todas as informações necessárias para elaboração da arquitetura de implementação; • Fazer a análise e definição da Arquitetura de Implementação, baseada nas melhores práticas de mercado em conjunto com a equipe da CONTRATANTE; • Análise e mitigação de riscos ao negócio; • Estimativa de impacto e janelas de indisponibilidade;	Obrigatório

Características		• Entrega da Arquitetura de Implementação para validação técnica da CONTRATANTE; • Elaborar o cronograma detalhado do projeto.	
	1.4	A CONTRATADA deverá configurar, instalar e testar, nas dependências do Data Center da CONTRATANTE, os produtos, conforme projeto de implantação elaborado pela CONTRATADA e aprovado pela equipe técnica da CONTRATANTE, apresentando junto a cada produto um documento com instruções passo-a-passo para a sua instalação física.	Obrigatório
	1.5	Os produtos fornecidos serão instalados e configurados em conformidade com o padrão da Rede IP Multisserviços da CONTRATANTE.	Obrigatório
	1.6	A CONTRATADA deverá instalar, configurar e testar os produtos para Data Center da CONTRATANTE. Estas ações deverão contemplar pelo menos as seguintes atividades: • Análise preliminar da topologia e operação atual da Rede IP Multisserviços da CONTRATANTE com vistas a seu aproveitamento na solução ofertada; • Completa instalação e configuração, testes em produção e ajustes de toda a solução ofertada; • Implementação, com a coleta de evidências, dos controles de requisitos de segurança da CONTRATANTE, que forem possíveis de serem aplicados nos equipamentos/produtos da solução ofertada; • Acompanhamento e homologação do ambiente de produção; • Documentação detalhada de todos os passos da instalação, configuração e ajustes, no ambiente de produção, a qual deverá ser entregue em meio impresso e em arquivo eletrônico no formato PDF antes da	Mínimo Obrigatório

		emissão do Atestado de Recebimento Definitivo a ser expedido pela CONTRATANTE.	
	1.7	Os trabalhos serão coordenados e acompanhados pelos analistas e técnicos da CONTRATANTE, devendo haver repasse de conhecimento durante a execução dos serviços.	Obrigatório
	1.8	A critério da CONTRATANTE, os serviços poderão ser executados fora do horário comercial e/ou em finais de semana ou feriados sem custo adicional para a CONTRATANTE, visando minimizar os transtornos aos usuários pela eventual indisponibilidade da rede.	Mínimo Obrigatório
	1.9	Para todos os efeitos, a conclusão dos serviços de instalação, configuração, testes em produção e ajustes será dada pela entrega da solução em pleno funcionamento, de acordo com as recomendações do(s) fabricante(s) e demais condições estabelecidas neste Edital.	Mínimo Obrigatório
	2.0	Repasse de conhecimento da solução ofertada item 1 – Lote 1, do tipo teórico e prático.	Obrigatório
	2.1	O(s) instrutor(es) deverá(ão) possuir conhecimentos comprovados na solução fornecida.	Obrigatório
	2.2	Deverá ser realizado no ambiente da CONTRATANTE, com material didático digital (PPT ou PDF, documentação do projeto e manuais de produto) fornecido pela CONTRATADA.	Mínimo obrigatório
	2.3	O repasse de conhecimento deverá ser realizado pela CONTRATADA para duas turmas, de 4 (quatro) vagas, para analistas e técnicos da CONTRATANTE, perfazendo um total mínimo de 8 (oito) horas por turma e deverá ser ministrado no turno matutino, ou vespertino, conforme a necessidade do Órgão/Entidade, em horário comercial e dias úteis contínuos.	Mínimo obrigatório
Repasse de conhecimento		O repasse de conhecimento compreenderá necessariamente os	

		seguintes tópicos: • Instalação, configuração e operação dos produtos; • Apresentação do Projeto da CONTRATANTE; • Descrição da arquitetura dos produtos; • Descrição do *software* disponíveis dos produtos; • Estratégias de implementação dos produtos; • Configuração e administração dos produtos.	Mínimo obrigatório
	2.5	É responsabilidade da CONTRATANTE zelar pelo comparecimento e assiduidade dos tecnicos/analistas à capacitação aplicada.	Obrigatório
	2.6	A CONTRATANTE poderá solicitar a repetição do repasse de conhecimento caso entenda que o mesmo não cumpriu os requisitos estipulados.	Mínimo obrigatório

1.1.4. **Lote 1 - Item 4 - Serviços de treinamento da solução ofertada:**

Lote 1 - Item 4 – Serviços de treinamento da solução ofertada			**Quantidade: 1 unidade**
Subitem		**Especificação**	**Exigência**
	1.0	Treinamento Oficial completo da solução ofertada item 1 – Lote 1, do tipo teórico e prático. Deverá contemplar o mesmo conteúdo indicado pelo fabricante da solução no treinamento oficial (ministrado pelo próprio fabricante ou por profissional certificado pelo mesmo). No caso de a solução ofertada ser uma atualização do ambiente utilizado pela SEFMG atualmente (*Checkpoint*), poderá ser ofertado um Treinamento de Atualização, fornecido pelo próprio fornecedor , tendo em vista o conhecimento técnico já adquirido nesta plataforma ao longo de anos de trabalho e o amplo conhecimento da ferramenta pelos Analistas de Sistemas, as políticas e regras já	Obrigatório

	implementadas e o conjunto de dados a serem aproveitados.	
1.1	Os instrutores deverão ser certificados pelo fabricante e possuir conhecimentos comprovados na solução fornecida.	Obrigatório
1.2	A CONTRATADA deverá apresentar certidão de capacidade técnica e documento comprobatório de parceria com o fabricante do produto e autorização para ministrar o Treinamento Oficial. Será aceito o fornecimento de treinamento oficial do fabricante, através da contratação de um Centro de Treinamentos Autorizado pelo fabricante.	Obrigatório
1.3	É obrigatório relacionar na proposta comercial a ementa do curso, carga horária e conteúdo programático.	Mínimo obrigatório
1.4	A CONTRATADA disponibilizará um laboratório que permita a simulação de ambientes com características similares aos propostos na solução implantada, possibilitando exercícios práticos de configuração dos produtos durante os módulos de capacitação em que tais atividades se apliquem. O ambiente de laboratório poderá ser montado em local disponibilizado pela CONTRATADA, em Belo Horizonte/MG, ou poderá estar nas dependências do fabricante e/ou fornecedor. Caso o laboratório esteja nas dependências do fabricante e/ou fornecedor, deverá ser acessado através de VPN/Internet, durante o período do treinamento, sendo de responsabilidade da CONTRATADA a disponibilização de local, em Belo Horizonte/MG, para realização do treinamento, bem como o acesso ao laboratório do fabricante e/ou fornecedor, com todos os recursos necessários (espaço físico, equipamentos, material didático, etc.). Na impossibilidade de o	Obrigatório

Características		treinamento ser feito de forma presencial, devido às condições sanitárias atuais causadas pelo pandemia de COVID, a CONTRATANTE poderá avaliar e aceitar que o treinamento seja feito de forma virtual, em que os técnicos a serem treinados deverão ter acesso à plataforma de treinamento do fornecedor ou do fabricante, mantendo-se as demais condições definidas nesta especificação.	
	1.4	O local do treinamento deverá ser disponibilizado pela CONTRATADA, na cidade de Belo Horizonte, devendo todos os custos (sala, instrutores, *desktop*, etc.) serem de responsabilidade da CONTRATADA.	Mínimo obrigatório
	1.5	O treinamento completo ou treinamento de atualização da solução ofertada deverá ser realizado pela CONTRATADA, em 2 (duas) turmas de 5 (cinco) vagas cada, para analistas e técnicos da CONTRATANTE, perfazendo um total de horas/aula de acordo com o recomendado pelo fabricante em seu treinamento, com o mínimo de: • 32 (trinta e duas) horas por turma, dividido em módulos de 4 (quatro) horas para o treinamento oficial; • 24 (vinte e quatro) horas por turma, dividido em módulos de 4 (quatro) horas para o treinamento de atualização. Além disso, deverá ser ministrado em dois turnos, com uma turma no período matutino e outra no período vespertino, conforme a necessidade da CONTRATANTE, em horário comercial e dias úteis contínuos, podendo a CONTRATADA concluir o treinamento em até 2 (duas) semanas consecutivas.	Mínimo obrigatório
	1.6	O treinamento estará centrado nas soluções fornecidas, privilegiando atividades práticas que permitam uma melhor fixação do aprendizado, que	Mínimo obrigatório

		possibilitem a equipe técnica da CONTRATANTE gerenciar e administrar a solução implantada.	
	1.7	A CONTRATADA deverá fornecer, no início de cada tópico, apostilas (em formato impresso ou digital) que abordem todo o conteúdo programático de acordo com o indicado pelo fabricante da solução no treinamento oficial, as quais poderão estar no todo ou em parte, em português e/ou inglês. O conteúdo do treinamento deverá abranger, pelo menos, os seguintes tópicos: instalação, configuração, operação, monitoramento, administração básica e avançada.	Obrigatório
	1.8	O início desta atividade, bem como o período e horário de realização, será definido pela CONTRATANTE em comum acordo com a CONTRATADA.	Obrigatório
	1.9	É responsabilidade da CONTRATANTE zelar pelo comparecimento e assiduidade dos treinandos à capacitação aplicada.	Obrigatório
	1.10	A CONTRATANTE poderá solicitar a repetição do treinamento caso entenda que o mesmo não cumpriu os requisitos estipulados.	Mínimo obrigatório

1.1.5. **Lote 2 - Item único - Servidor para solução *Firewall*:**

Lote 2 - Item único – Especificação Servidor para Solução			**Quantidade: 4 unidade**
Subitem		**Especificação**	**Exigência**
Descrição	1.0	Aquisição de servidores para solução de segurança com as características técnicas e requisitos gerais relacionados neste documento.	Obrigatório
CPU	2.0	02 (dois) Processadores compatíveis com arquitetura *Intel Xeon* de no minimo 3,3GHz (frequência baseada em processador e não em frequência turbo max), 12 núcleos/24 segmentos e observado o desempenho especificado no subitem 11	Mínimo obrigatório

CPU		desta especificação técnica.	
	2.1	O processador deverá ser da última geração disponibilizada pelo fabricante no Brasil; O modelo do servidor ofertado deve possuir o índice auditado, no sítio eletrônico oficial SPEC® - http://www.spec.org.	Obrigatório
Placa Mãe	3.0	Suporte para o(s) processador(es) citado(s) no subitem 2.0.	Obrigatório
	3.1	*Clock* do barramento de sistemas compatível com o *clock* do processador.	Obrigatório
	3.2	Barramento PCI.	Obrigatório
	3.3	2 (dois) *slots* de expansão PCIe 3.0.	Obrigatório
Memoria	4.0	256 GB (4x64 gigabytes ou 8x32 gigabytes) 2933MT/s, *Dual Rank*, BCC.	Mínimo obrigatório
	4.1	2933MT/s RDIMMs.	Mínimo obrigatório
Interfaces	5.0	4 portas USB, com pelo menos duas USB 3.0.	Mínimo obrigatório
	5.1	1 interface serial RS-232.	Mínimo obrigatório
	5.2	Controladora de vídeo (1 conector VGA).	Mínimo obrigatório
Armazenamento Interno	6.0	2 (dois) disco SAS com velocidade de rotação 10k ou 15k ou SATA/SAS SSD, com capacidade mínima de 1.000 GB (Um mil gigabytes) cada disco.	Mínimo obrigatório
	6.1	Controladora RAID PERC H730P, 2GB NV *Cache*, *Minicard.*	Mínimo obrigatório
Rede	7.0	Placa auxiliar de rede Intel X710 4 portas 10Gbps (SFP+) prontas para uso, DA/SFP+, *Ethernet*. Todos os *transceivers* e SFPs, devem ser fornecidos. As interfaces deverão utilizar driver IXGBE compatível com *multi-queue* de 16 filas.	Obrigatório
		2 (duas) portas/*interfaces* 1/10 Gigabit Ethernet 1000Base-	

	7.1	T/10GBase-T, padrões IEEE 802.3, full-duplex, *autosensing*, conector RJ-45 fêmea, configuráveis por *software*, *led* indicativo do *status* da conexão.	Mínimo obrigatório
Software	8.0	Sem sistema operacional.	Obrigatório
Alimentação	9.0	Fonte de alimentação redundante "*hot swappable*".	Obrigatório
	9.1	Tensão de 127/220 V e frequência de 60 Hz.	Obrigatório
Gerência	10.0	Suporte a SNMP.	Obrigatório
	10.1	Acesso remoto as funções de vídeo, teclado e mouse (KVM) através de interface de gerenciamento Ethernet 10/100 Mbps.	Obrigatório
Desempenho	11.0	O equipamento ofertado deverá ter desempenho '*SPEC CPU2017 Integer Rate base*', **mínimo de190 (cento e noventa)**, a ser comprovado através de informações publicadas no *site* www.spec.org ("*All SPEC CPU2017 Results Published by SPEC*" com detalhamento em '*SPEC CPU2017 Integer results*' - http://www.spec.org/cgi-bin/osgresults?conf=rint2017" O índice poderá ser estimado para equipamentos da mesma família para os quais não tenha sido realizado o *benchmark* em questão, mediante utilização de índices de *performance* relativa ou qualquer outra informação que permita correlacionar a capacidade de processamento de equipamentos similares.	Obrigatório
Característica Física	12.0	Possuir dimensões e acessórios que possibilitem sua fixação em *rack* padrão de 19 polegadas com organizador de cabos.	Obrigatório
	12.1	O gabinete deverá ter no máximo 1 RU.	Obrigatório
Certificações	13.0	O equipamento deverá ter aprovação das normas FCC part 15.	Obrigatório
		O equipamento deverá possuir	

Documentação	14.0	manual (em português ou inglês) de todos os dispositivos e *software* que acompanham o conjunto.	Obrigatório
	14.1	As informações sobre o atendimento dos requisitos constantes desta especificação técnica deverão estar claramente informadas no catálogo do equipamento publicado pelo fabricante.	Obrigatório
	14.2	Deverá ser provida toda a documentação técnica que possibilite a averiguação de conformidade com estas especificações. Poderão ser utilizados na proposta da licitante o uso de *datasheets*, manuais e páginas de Internet mantidas pelo fabricante.	Obrigatório
Acessórios	15.0	Os servidores deverão vir acompanhados dos trilhos para montagem em *rack*, bem como todos os suportes de guia de metal de sustentação dos cabos de rede e de monitor de vídeo além, dos cabos de alimentação dos servidores.	Obrigatório
	16.0	Todos os componentes integrantes do equipamento devem possuir garantia integral, original de fábrica, contra defeitos de fabricação, por período não inferior a 48 (quarenta e oito) meses contados a partir da data de expedição do Termo de Recebimento Definitivo, sem ônus adicional para a CONTRATANTE.	Mínimo obrigatório
	16.1	A prestação de serviços de suporte técnico, correção de problemas e atualização de versões (manutenção) relativa a o s *software* fornecidos, incluindo para o Sistema Operacional, deve ser pelo período mínimo de 48 (quarenta e oito) meses, sem ônus adicional para a CONTRATANTE.	Mínimo obrigatório
		A CONTRATADA deverá identificar, habilitar e manter um canal de contato técnico junto ao fabricante para	

16.2	acesso direto da CONTRATANTE por meio de seus representantes credenciados. Este canal de contato deverá ser configurado para acesso direto a técnicos habilitados do fabricante visando à resolução de problemas e/ou orientação direta aos técnicos da CONTRATANTE.	Mínimo obrigatório
16.3	A CONTRATADA deverá fornecer lista com todos os dados necessários para abertura de chamados técnicos (por exemplo: códigos de identificação dos equipamentos, descrição, versão de firmware, etc.).	Obrigatório
16.4	O atendimento de suporte técnico deverá ser via “Central de Atendimento ao Usuário” para abertura de chamados e resolução de problemas tipo 24x7 (vinte e quatro horas por dia, sete dias por semana).	Obrigatório
16.5	A CONTRATADA deverá substituir todos os componentes (exceto os gabinetes) do equipamento fornecido e já instalado por outros iguais ou superiores, em perfeito estado de funcionamento, no prazo de 60 (sessenta) dias após solicitação da CONTRATANTE, na ocorrência de mais de 4 (quatro) eventos que totalizem 32 (trinta e duas) horas de indisponibilidade e que comprometam o seu perfeito funcionamento dentro de um período contínuo qualquer de 30 (trinta) dias.	Obrigatório
16.6	A substituição não acarretará ônus para a CONTRATANTE e não eximirá o fornecedor das penalidades previstas.	Obrigatório
16.7	A assistência técnica utilizará apenas peças e componentes originais, salvo nos casos fundamentados por escrito e aceitos pela CONTRATANTE.	Obrigatório
	Para complementar a garantia oferecida pelo fabricante, a CONTRATADA deverá prestar	

Garantia	16.8	serviço de assistência técnica. Este serviço será prestado durante a vigência da garantia, que é de 48 (quarenta e oito) meses, e garantirá à CONTRATANTE o cumprimento de limites para o prazo de atendimento e de solução do problema exigidos. • O prazo de atendimento para chamados técnicos relativos a eventos de indisponibilidade ou manutenção de *hardware* será do tipo 24x7 (7 dias por semana, 24 horas por dia), com atendimento em até 4 (quatro) horas corridas após o chamado e solução do problema em até 48 (quarenta e oito) horas corridas. O prazo de atendimento é dado pelo tempo decorrido entre a abertura do chamado pela CONTRATANTE e o início da atividade de diagnóstico pela CONTRATADA. A atividade será considerada iniciada a partir da chegada do técnico da CONTRATADA na Superintendência de Tecnologia da Informação ou unidade equivalente da CONTRATANTE, ou a partir do horário do acesso remoto registrado no log do equipamento ou ainda a partir do contato efetuado por telefone pelo técnico da CONTRATADA, a critério da CONTRATANTE. • O prazo de solução para evento de indisponibilidade será contado a partir da abertura do chamado pela CONTRATANTE. • Entende-se como solução do problema: 1. Em caso de defeito d e *hardware*, a correção do defeito ou o retorno do acesso aos dados; 2. Em caso de	Obrigatório

	problemas em *software* ou microcódigo, a correção do defeito ou implementação de solução de contorno para o retorno do acesso aos dados, desde que a correção definitiva ocorra posteriormente, dentro de um prazo acordado entre as partes, em função da complexidade da ocorrência.	
16.9	Ao final de cada atendimento resultante de abertura de chamado, por parte da área de TI da CONTRATANTE, a CONTRATADA deverá emitir laudo técnico contendo no mínimo: • Data e hora do chamado; • Data e hora do início e do término do atendimento; • Identificação do defeito; • Identificação unívoca do equipamento (componente que apresentou problemas); • Providências adotadas.	Mínimo obrigatório
16.10	Atualização de *firmware* de todos os componentes da solução durante todo o prazo de garantia do equipamento, sem custo adicional para a CONTRATANTE.	Obrigatório
16.11	Caso o fornecedor entenda necessária a realização de serviços de manutenção preventiva, estes deverão ser agendados com antecedência mínima de 5 (cinco) dias úteis.	Obrigatório
16.12	Alterações nas configurações realizadas durante a execução desta assistência técnica deverão ser atualizadas na documentação especificada.	Obrigatório
16.13	A manutenção e troca de peças deverão ser executadas por técnicos certificados pelo	Obrigatório

	16.13	fabricante, no local onde se encontra o equipamento (*on site*).	Obrigatório
Suporte técnico	17.0	Deverá ser prestado incondicionalmente, sem custos adicionais, acesso liberado ao sítio na Internet do fabricante, onde seja possível encontrar os seguintes itens de suporte mínimo: • Possibilitar *download* de atualizações de todas as versões de *software* fornecidos; • Possibilitar o acesso a *drivers* de dispositivos, sistemas embarcados – componentes, interfaces de rede, controladoras, etc.; • Novas versões de *software* lançadas durante o período de garantia, possibilitando acesso de forma *on-line* ou efetuar *download* de *software*, manuais ou guias de referência técnicas de componentes dos componentes de *software* necessários ao funcionamento da solução fornecida.	Mínimo obrigatório
	18.0	Este serviço consiste na colocação do equipamento em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no edital e seus Anexos, e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da CONTRATANTE.	Obrigatório
	18.1	A instalação física do equipamento será realizada pelo fornecedor, com acompanhamento de uma equipe destacada pela CONTRATANTE.	Obrigatório
	18.2	A instalação, configuração e testes do equipamento deverão ser feitos com o acompanhamento de técnicos da CONTRATANTE, visando ao repasse de conhecimento e	Obrigatório

		observados os padrões segurança da CONTRATANTE.	
Instalação	18.3	O equipamento deverá estar com todas as funcionalidades e recursos de *hardware* e *software* solicitados disponíveis e configurados. Os sistemas de gerenciamento e de acionamento automático de suporte técnico também deverão estar ativos e em pleno funcionamento, levando em consideração todas as características solicitadas.	Obrigatório
	18.4	A instalação e a configuração do equipamento deverão ocorrer preferencialmente em dias úteis, de 9 às 17 horas, ficando a cargo da CONTRATANTE a definição dos horários para configuração do equipamento em produção. Atividades a serem realizadas fora deste horário estarão sujeitas à aprovação prévia da equipe da área de TI da CONTRATANTE.	Obrigatório
	18.5	Todos os componentes de *hardware* e *software* deverão funcionar em conjunto, simultaneamente, sem conflitos, de forma integrada entre eles e o ambiente de infraestrutura de TI da CONTRATANTE.	Obrigatório
Capacitação técnica	19.0	Fornecer capacitação dos técnicos da CONTRATANTE no modelo "*hands-on*" para a instalação e configuração do equipamento, provendo os técnicos da área de TI da CONTRATANTE a capacidade de gerenciamento e manutenção da solução em todas as suas funcionalidades, inclusive aquelas não expressamente exigidas como requisitos, mas disponíveis na solução ofertada.	Obrigatório

2. DOS LOTES:

2.1. DO AGRUPAMENTO DE ITENS EM LOTES:

2.1.1. Não se observa, nesta aquisição, a possibilidade de divisão de itens em lotes distintos, além dos 2 (dois) lotes propostos, considerando que o objeto é composto de itens de soluções de mesma natureza e guardam relação entre si. Essa aglutinação teve vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da

competitividade, sem perda da economia de escala, de forma mais vantajosa ao Estado.

2.2. **LOTES EXCLUSIVOS PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE:**

2.2.1. Considerando-se que o valor de referência desta aquisição ultrapassa R$ 80.000,00 (oitenta mil reais), não há a possibilidade de divisão em mais lotes, além do que foi proposto não encontramos a possibilidade de aplicação do disposto no Art. 8º do Decreto nº 47.437, de 26 de junho de 2018 e, portanto, estabelecer a exclusividade de participação no processo apenas a fornecedores enquadrados como microempresas e empresas de pequeno porte. Entendemos, dessa forma, que o tratamento diferenciado e simplificado para as microempresas e empresas de pequeno não será vantajoso e poderá representar prejuízo ao conjunto do objeto a ser adquirido.

2.2.2. Ademais, quanto à participação exclusiva de ME/EPP, informamos que, quando da consulta para a formação dos preços de referência, não localizamos um mínimo de 3 (três) fornecedores competitivos enquadrados como microempresas e empresas de pequeno porte, sediados local ou regionalmente e capazes de cumprir as exigências estabelecidas no instrumento convocatório. Dessa forma, entendemos que delimitar participação exclusiva de ME/EPP para o presente processo poderá trazer prejuízos ao certame.

3. JUSTIFICATIVA DA CONTRATAÇÃO:

Nos últimos anos a Secretaria de Estado de Fazenda de Minas Gerais vem desenvolvendo aplicações cada vez mais robustas e que não podem sofrer interrupção ou intermitência, por serem de fundamental importância para o funcionamento de serviços essenciais desta Secretaria, utilizados por empresas e cidadãos, sob pena de a sociedade ficar sem acesso a sistemas empregados cotidianamente, como SIARE, SICAF, Cadastro Sincronizado, NFe, NFC-e, PTA-e e Nota Fiscal Mineira, etc.

Atualmente as instituições que disponibilizam serviços críticos para seus usuários na internet devem atender a um alto padrão de confiabilidade e segurança em relação a uma variedade de ameaças em constante evolução. À medida que sua infraestrutura de rede migra de redes distintas e proprietárias para redes convergentes baseadas em Protocolo de Internet (IP), eles estão sob risco crescente de ameaças cibernéticas. Por outro lado, com a crescente adoção da computação em nuvem, os serviços baseados na Internet são cada vez mais críticos tanto para as empresas como para as organizações governamentais.

Para sustentar este crescimento rápido, a SEF/MG busca a cada dia uma rede mais confiável, de alto desempenho e mais fácil de gerenciar. A partir de 2008, quando foi feita uma revisão da infraestrutura de redes para convergir voz e dados em uma única rede, fez-se necessária uma solução de segurança com desempenho e estabilidade para lidar com o tráfego combinado. Naquela época, os *firewalls* existentes eram insuficientes para atender às demandas de segurança. A partir de então, a SEF/MG se viu obrigada a substituí-los e simultaneamente, adotar medidas mais concretas para ampliar a segurança de rede a todas as suas unidades remotas. Enquanto suas unidades tinham conexões diretas à rede, alguns órgãos e usuários externos tinham sido deixados fora dela, somente com acesso à Internet via VPN. A SEF/MG substituiu completamente seus *firewalls*, optando por uma solução de segurança fornecida pela empresa *CheckPoint* para maximizar a disponibilidade e o desempenho de seu *gateway* de segurança e distribuir o tráfego entre dois *gateways* no perímetro de sua rede central. Essa solução proporcionou um maior *throughput* juntamente com a tão necessária redundância, além de possibilitar uma simplificação no gerenciamento da solução e a utilização de uma maneira segura de acessar os aplicativos e as informações corporativas por meio de conexões IPSec VPN *site-a-site*.

Em 2013 a SEF deparou-se com a necessidade de oferecer aos seus usuários móveis acesso remoto com o mesmo nível de segurança disponibilizado em seu ambiente

operacional e com controle de acesso, autenticação de usuários e encriptação em um equipamento de fácil instalação e gerenciamento. Diante dessas demandas e para cobrir as lacunas que a solução da época não dispunha sobre modelo de acesso, fez-se necessária a migração da solução *CheckPoint* (*Hardware e Software*) para uma solução mais robusta e que tratava as questões de segurança da informação em toda a sua amplitude, em conformidade com a politica de segurança vigente da SEF/MG. A migração da solução para um modelo de equipamento do mesmo fabricante visou a manutenção do padrão tecnológico empregado a fim de preservar investimentos em capacitação e formação de pessoal e com a finalidade de garantir padronização.

Recentemente, a SEF foi informada pela empresa que faz o suporte técnico da solução *Checkpoint* em uso que, para o modelo em utilização, o contrato de suporte não poderá mais ser renovado. Diante da criticidade dessa solução dentro do ambiente de TI, faz-se necessário que seja adquirida nova solução, visto que é absolutamente necessário que o *firewall* tenha atualizações constantes a fim de mitigar as ameaças que aparecem frequentemente.

A fim de possibilitar o aproveitamento das licenças utilizadas nos *appliances* da *Checkpoint* de propriedade da SEF/MG, optou-se por aceitar a possibilidade de upgrade dessas licenças, a serem instaladas em equipamentos servidores que serão adquiridos especificamente para essa finalidade.

Por fim, cumpre mencionar que as especificações técnicas constantes deste processo foram definidas com base nas necessidades da SEF/MG e nas características dos produtos disponíveis no mercado. Os estudos realizados para elaboração da especificação, bem como as aquisições e remanejamentos permitirão melhor uso dos recursos do erário, melhorando a relação de custo/benefício desse gasto, atendendo melhor, dessa maneira, ao interesse público.

Frisamos, mais especificamente quanto à adequação da demanda ao plano de contingenciamento de gastos, em essência ao Decreto nº 48.205/2021, que prorroga o prazo de vigência do estado de calamidade pública de que trata o art. 1º do Decreto 47.891/2020, até 31/12/2021, no âmbito de todo o território do Estado, que tem como objetivo essencial direcionar ações gerais para mitigar os impactos financeiros causados pela epidemia de doença infecciosa viral respiratória causada pelo agente Coronavírus – COVID-19, que os impactos trazidos com a despesa desta contratação encontram-se limitados aos créditos orçamentários previstos em programação orçamentária e financeira do Estado de Minas Gerais. Vale acrescentar que a solução contemplada nesta contratação, é essencial à proteção do ambiente que mantém o funcionamento das aplicações críticas disponibilizadas aos funcionários da SEF/MG e a toda a sociedade mineira. A não aquisição dessa nova solução poderia, portanto, trazer graves prejuízos à Administração Pública e aos contribuintes, o que, entendemos, s.m.j., poderia trazer impactos mais severos para a situação reconhecida de calamidade pública.
Diante do exposto, recomendamos a aquisição da solução de segurança com funcionalidades de Firewall, Sistema de Prevenção de Intrusão (IPS), Redes Virtuais Privadas (VPN), Controle de Aplicações e Ameaças, Filtro de URL e Protocolo de Qualidade de Serviço (QoS) Integrados e servidores para substituição dos equipamentos ora em uso na SEF-MG, assim como serviços de instalação, suporte técnico, atualização, garantia e treinamento para o ambiente de Data Center, conforme especificações, exigências e quantidades estabelecidas neste documento.

4. JUSTIFICATIVA DA MODALIDADE:

4.1. Sugere-se a modalidade de Pregão Eletrônico por se tratar de aquisição de bens e serviços de natureza comum, fundamentado em dois fatores: (I) a possibilidade jurídica de caracterização do objeto da licitação de aquisição de bens e serviços comuns, nos termos da Lei Federal nº 10.520/2002, da Lei Estadual n°. 14.167/ 2002 e do Decreto Estadual nº 48.012/2020; e (II) a necessidade de se contratar aquele que oferecer o menor valor pelo bem, dentro dos parâmetros objetivamente fixados neste termo.

5. DA PARTICIPAÇÃO DE CONSÓRCIOS:

5.1. Sendo ato discricionário da administração, não será permitida a participação de empresas reunidas em consórcio, considerando que as empresas que atuam no mercado têm condições de fornecer o objeto desta aquisição de forma independente. Como não há necessidade de participação de empresas reunidas em consórcio para o fornecimento dos bens e prestação de serviços, objeto desta aquisição, esta equipe entende que permitir esse tipo de participação poderia trazer prejuízos à competição do certame licitatório.

6. QUALIFICAÇÃO TÉCNICA:

6.1. Para os lotes 1 e 2: Atestado(s) de Capacidade Técnica da licitante, emitido(s) por entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou empresa privada que comprove, de maneira satisfatória, a aptidão para desempenho de atividades pertinentes ao objeto a ser licitado, comprovando o fornecimento prévio de produtos e/ou serviços similares aos especificados no objeto desta aquisição, contemplando garantias compatíveis às exigidas em relação a prazos, níveis de serviços e características. Os atestados deverão conter:

6.1.1. Nome empresarial e dados de identificação da instituição emitente (CNPJ, endereço, telefone);

6.1.2. Local e data de emissão;

6.1.3. Nome, cargo, telefone, e-mail e a assinatura do responsável pela veracidade das informações;

Justificativa: Considerando que a implementação da solução de segurança a ser instalada no *core* do ambiente de TI desta Secretaria demanda serviços altamente especializados e que dependem da expertise dos técnicos, com total apoio e suporte do fabricante da solução, é imprescindível que o fornecedor comprove sua aptidão para os serviços por meio da apresentação de Atestado de Capacidade Técnica, confirmando o prévio fornecimento de serviços similares ao ora pretendidos pela Administração Pública. O risco de não exigência desse atestado pode colocar em risco um ambiente de TI extremamente crítico, com consequências econômicas incalculáveis para o Estado de Minas Gerais, contribuintes mineiros e toda a sociedade, que depende das aplicações hospedadas no Data Center da SEF, uma vez que essa solução visa proteger o Data Center de ataques eletrônicos, o que ocorre rotineiramente.

7. CRITÉRIOS DA ACEITABILIDADE DA PROPOSTA:

7.1. Os produtos a serem ofertados deverão ser novos e não poderão estar fora de linha de produção do fabricante na data da entrega, fato que deverá ser comprovado pela CONTRATADA, caso solicitado pela Superintendência de Tecnologia da Informação – STI, não denotando uso anterior ou recondicionamento e entregues em suas embalagens originais lacradas.

7.2. É condição indispensável e obrigatória, a apresentação pelo fornecedor vencedor, das especificações e características detalhadas do serviço ofertado, incluindo a marca, modelo e configurações dos produtos e das ampliações.

7.3. Os licitantes deverão anexar, via sistema eletrônico, sob pena de não aceitabilidade da proposta, os documentos abaixo relacionados:

7.3.1. Para a aceitabilidade da proposta, a pregoeira poderá solicitar, como diligência, que o licitante detentor do melhor lance, por Lote, apresente planilha de especificações técnicas para o item 1 do lote 1 e item único do lote 2, conforme Anexo II, acrescida de uma coluna à direita, denominada “ofertado”, onde deverá constar para cada subitem a especificação precisa ofertada (caso superior à mínima exigida) ou apenas "SIM” (caso coincida com a característica solicitada), bem como o número da página do catálogo ou manual do produto que comprove o atendimento à requisição do subitem.

7.3.2. O fornecedor deverá indicar o endereço eletrônico do sítio do fabricante onde, por acesso sem restrição de credenciais (sem a

necessidade de usuário e senha) ou qualquer outro método de autenticação, possam ser consultados os catálogos/manuais contendo as especificações técnicas do produto/serviço, que confirmem as funcionalidades exigidas.

7.3.3. No caso de não haver catálogo/manual disponível na Internet, poderá ser encaminhado, juntamente com a proposta, catálogo original, com apresentação nítida e legível que permita a identificação do produto.

7.3.4. Caso no catálogo/manual constem diversos modelos, o fornecedor deverá identificar/destacar qual a marca/modelo do produto ofertado.

7.3.5. Quando o catálogo/manual for omisso na descrição de algum item da composição original do produto/serviço ofertado, o fornecedor deverá anexar Declaração Complementar ao catálogo/manual, com descrição da especificação faltante, sem que haja mudança substancial que venha a alterar as características originais do produto.

8. DA APRESENTAÇÃO DE AMOSTRAS:

8.1. Não será exigida a apresentação de amostras.

9. DA EXECUÇÃO DO OBJETO:

9.1. **Prazo de Entrega:**

9.1.1. **Para o item 1 do lote 1**: até 10 (dez) dias úteis, contados a partir da emissão do Termo de Recebimento Definitivo do item único do lote 2.

9.1.2. **Para o item 2 do lote 1:** imediatamente, a contar da expedição do Termo de Recebimento Definitivo para o item 1 do lote 1 pela SEF.

9.1.3. **Para o item 3 do lote 1**: início em até 15 (quinze) dias úteis, contados do Recebimento Provisório do item 1 do lote 1, e término em até 60 (sessenta) dias úteis após o início dos serviços de instalação.

9.1.4. **Para o item 4 do lote 1**: até 60 (sessenta) dias úteis contados da expedição do Termo de Recebimento Definitivo para o item 1 do lote 1.

9.1.5. **Para o item único do lote 2**: os equipamentos deverão ser entregues em até 45 (quarenta e cinco) dias, contados da emissão da Nota de Empenho.

9.1.6. Devidamente justificado e antes de finalizado o prazo de entrega, o fornecedor do produto poderá solicitar prorrogação da entrega, ficando a cargo da área demandante aceitar a solicitação, desde que não haja prejuízo no abastecimento da rede.

9.2. **Do Local e Horário de Entrega:**

9.2.1. Os materiais deverão ser entregues no seguinte endereço: Rua da Bahia, nº 1816, 1º Subsolo, STI, Bairro de Lourdes, Belo Horizonte - MG, no horário de 08:00 às 18:00, de segunda a sexta-feira.

9.3. **Condições de recebimento:**

9.3.1. Os produtos serão recebidos:

9.3.1.1. **Para o item 1 do lote 1**:

9.3.1.1.1. Provisoriamente, quando se verificar a disponibilização das licenças de *software* da solução ofertadas, para efeito de posterior verificação da conformidade do produto com a especificação, oportunidade em que se observarão apenas as informações constantes da fatura e descrição do produto, em confronto com a respectiva Nota de Empenho;

9.3.1.1.2. Definitivamente, com a emissão do Termo de Recebimento Definitivo, o que ocorrerá após a verificação da

qualidade e quantidade de licenças e consequente aceitação da solução, que deverá acontecer em até 10 (dez) dias úteis, contados da finalização dos Serviços de instalação, configuração, testes em produção e ajustes dos equipamentos/produtos e repasse de conhecimento, objeto do item 3 do lote 1.

9.3.1.2. **Para o item 2 do lote 1**:

9.3.1.2.1. O aceite do objeto será realizado mediante ateste da nota fiscal/fatura correspondente, pelo servidor designado pela SEF/MG para esse fim. Para a efetivação do ateste, será necessário comprovar, por declaração do fabricante ou por meio de acesso ao site do fabricante da solução ou através do próprio *software*, o período que se encontra ativo o serviço em nome da CONTRATANTE.

9.3.1.3. **Para o item 3 do lote 1**:

9.3.1.3.1. Definitivamente, mediante ateste da nota fiscal/fatura correspondente, após a emissão do Termo de Recebimento Definitivo do item 1 do lote 1, quando da verificação da qualidade dos serviços prestados e atendimento aos itens das especificações.

9.3.1.4. **Para o item 4 do lote 1**:

9.3.1.4.1. Definitivamente, mediante ateste da nota fiscal/fatura correspondente, o que ocorrerá após a verificação da qualidade dos serviços prestados e atendimento aos itens da especificação.

9.3.1.5. **Para o item único do lote 2**:

9.3.1.5.1. Provisoriamente, no momento da entrega dos produtos, para efeito de posterior verificação da conformidade do produto com a especificação. Na oportunidade se observarão apenas as informações constantes da fatura e descrição do produto, em confronto com a respectiva Nota de Empenho;

9.3.1.5.2. Definitivamente, com a emissão do Termo de Recebimento Definitivo, o que ocorrerá após a verificação da qualidade e quantidade de servidores, assim como a consequente aceitação da solução, que deverá acontecer em até 10 (dez) dias úteis, contados da finalização dos serviços de instalação.

9.3.2. O descarregamento do produto ficará a cargo do fornecedor, devendo ser providenciada a mão-de-obra necessária.

9.3.3. O recebimento/aprovação do(s) produto(s) pela Secretaria de Estado de Fazenda de Minas Gerais não exclui a responsabilidade civil do fornecedor por vícios de quantidade ou qualidade do(s) produto(s) ou disparidades com as especificações estabelecidas, verificadas posteriormente, garantindo-se à Administração as faculdades previstas no art. 18 da Lei n.º8.078/90.

9.3.4. O Fornecedor deverá apresentar comprovação de que está autorizado pelo fabricante da solução ofertada a vender e prestar os serviços de suporte.

9.4. **Emissão do Termo de Recebimento Definitivo:**

9.4.1. O Termo de Recebimento Definitivo será expedido pela equipe técnica designada pela CONTRATANTE no prazo de até 10 (dez) dias úteis após a conclusão das atividades abaixo:

9.4.1.1. disponibilização dos serviços contratados, incluindo os serviços de instalação e configuração dos equipamentos instalados e repasse de conhecimentos;

9.4.1.2. apresentação teórica e prática concluída;

9.4.1.3. documentação entregue, bem como os procedimentos a

serem seguidos para abertura de chamados técnicos;

9.4.1.4. relatório de acompanhamento de produção, com esse ambiente estável por, no mínimo, 2 (dois) dias úteis;

9.4.1.5. entrega de cópia do contrato, autenticada por cartório competente ou por servidor da administração, celebrado entre a CONTRATADA e o fabricante do equipamento, ou declaração emitida pelo fabricante do equipamento ratificando a garantia e os níveis de serviço exigidos.

9.4.2. O Termo de Recebimento Definitivo somente será expedido após minuciosa aferição de conformidade dos produtos e/ou serviços fornecidos, bem como de toda a documentação especificada neste Termo de Referência e é o documento que atesta o início da prestação do serviço ou entrega do produto objeto deste Termo de Referência

9.4.3. É facultado à CONTRATADA se fazer representar por um técnico de sua equipe perante a equipe técnica da CONTRATANTE durante os procedimentos de aferição e recebimento definitivo dos serviços fornecidos.

9.5. **Cronograma físico-financeiro:**

9.5.1. Para todos os itens, objeto desta contratação, o pagamento será único e integral.

10. DO PAGAMENTO:

10.1. O pagamento será efetuado através do Sistema Integrado de Administração Financeira - SIAFI/MG, por meio de ordem bancária emitida por processamento eletrônico, a crédito do beneficiário em um dos bancos que o fornecedor indicar, no prazo de até **30 (trinta)** dias corridos, contados a partir da data final do período de adimplemento a que se referir, com base nos documentos fiscais devidamente conferidos e aprovados pela CONTRATANTE.

11. DO CONTRATO:

11.1. Encerrado o procedimento licitatório, o representante legal do licitante declarado vencedor será convocado para firmar o termo de contrato, aceitar ou retirar o instrumento equivalente, de acordo com os art. 62, da Lei 8.666/93 e art. 4º, XXI, da Lei 10.520/2002.

11.2. O contrato terá vigência por 12 (doze) meses, a partir da publicação de seu extrato no Diário Oficial do Estado de Minas Gerais. No entanto, haverá possibilidade de prorrogação do item 2 do lote 1 que trata da prestação de serviços de suporte, garantia e atualização da solução *Firewall,* podendo ser prorrogado por idêntico período até o limite máximo de 48 (quarenta e oito) meses, mediante celebração de termos aditivos, conforme dispõe o art. 57, IV da lei n.º 8.666/93.

11.3. Durante o prazo de vigência, o preço contratado no item 2 do lote 1 poderá ser reajustado monetariamente com base no IPCA, observado o interregno mínimo de 12 meses, contados da apresentação da proposta, conforme disposto na Resolução Conjunta SEPLAG/SEF nº8.898/ 2013 e nos arts. 40, XI, e 55, III**,** da Lei nº 8.666/93, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

11.4. Os efeitos financeiros retroagem à data do pedido apresentado pela contratada.

12. PROCEDIMENTOS DE FISCALIZAÇÃO E GERENCIAMENTO DA RELAÇÃO JURÍDICA:

12.1. Atendendo às exigências contidas no inciso III do art. 58 e §§ 1º e 2º, do artigo 67 da Lei nº. 8.666 de 1993, serão designados pela autoridade competente, agentes para acompanhar e fiscalizar o contrato, como representantes da Administração.

12.1.1. Izabelle Passos Gouvêa - Masp: 752.556-1(titular); e

12.1.2. Sílvio Henrique Araújo Couto - Masp 669.259-4(suplente).

12.2. Em caso de eventual irregularidade, inexecução ou desconformidade na execução do contrato, o agente fiscalizador dará ciência à CONTRATADA, por escrito, para adoção das providências necessárias para sanar as falhas apontadas.

12.3. A fiscalização de que trata esta cláusula não exclui, nem reduz a responsabilidade da CONTRATADA por quaisquer irregularidades, inexecuções ou desconformidades havidas na execução do objeto, aí incluídas imperfeições de natureza técnica ou aquelas provenientes de vício redibitório, como tal definido pela lei civil.

12.4. A CONTRATANTE reserva-se o direito de rejeitar, no todo ou em parte, o objeto da contratação, caso o mesmo afaste-se das especificações do Edital, seus anexos e da proposta da CONTRATADA.

12.5. Constatada a ocorrência de descumprimento total ou parcial do contrato, que possibilite a aplicação das sanções previstas neste instrumento, deverão ser observadas as disposições do art. 40 (e seguintes) do Decreto Estadual nº 45.902, de 27 de janeiro de 2012.

12.6. As decisões e providências que ultrapassarem a competência do Fiscal do Contrato serão encaminhadas à autoridade competente da CONTRATANTE para adoção das medidas convenientes, consoante disposto no § 2º do art. 67, da Lei nº. 8.666/93.

12.6.1. Caberá ao gestor os controles administrativos/financeiros necessários ao pleno cumprimento do contrato.

13. DOTAÇÃO ORÇAMENTÁRIA:

13.1. As despesas com esta contratação serão acobertadas pelas dotações orçamentárias 1191 04 126 115 2052 0001 4490 4006 e 1191 04 126 115 2052 0001 4490 5207, fontes 10.1 e/ou 48.1, 1191 04 126 115 2052 0001 3390 3921, 1191 04 126 115 2052 0001 3390 4002 e 1191 04 126 115 2052 0001 3390 3953 fonte 10.1, consignadas no orçamento em vigor e seus créditos suplementares, aprovada pela Lei 23.751, de 30 de dezembro de 2020, e quanto aos exercícios subsequentes, pelas dotações próprias que forem fixadas nos respectivos orçamentos.

14. DAS GARANTIAS:

14.1. Garantia financeira da execução:

14.1.1. No que se refere ao item 2 do Lote 1, o adjudicatário prestará garantia de execução do contrato, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e por 90 (noventa) dias após o término da vigência contratual, em valor correspondente a 5% do valor total referente ao item 2 do Lote 1.

14.1.1.1. Tal exigência se justifica em vista de haver previsão de pagamento em parcela única para a contratação e o item 2 do Lote 1 corresponde ao único item do processo que terá execução contínua durante a vigência do contrato. Os demais itens serão pagos após a entrega.

14.1.2. No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério da CONTRATANTE, contados da assinatura do contrato, a CONTRATADA deverá apresentar comprovante de prestação de garantia, somente para o item 2 do lote 1, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

14.1.2.1. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de três décimos por cento por dia (0,3%), até o trigésimo dia de atraso, do valor total do contrato.

14.1.2.2. O atraso superior a 30 (trinta) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas,

conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.

14.1.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

14.1.3.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

14.1.3.2. prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

14.1.3.3. multas moratórias e punitivas aplicadas pela Administração à CONTRATADA; e

14.1.3.4. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela CONTRATADA, quando couber.

14.2. **Garantia do produto/serviço: fabricante, garantia legal ou garantia convencional:**

14.2.1. Garantia legal estabelecida pelo Código de Defesa do Consumidor (CDC) de (30 dias - produtos não-duráveis) ;(90 dias - produtos duráveis) a partir da data de recebimento do produto, sem prejuízo de outra garantia complementar fornecida pelo licitante/fabricante em sua proposta comercial.

14.2.2. A garantia contra defeitos, para o item 1 do lote 1 será de 12 (doze) meses, contados a partir da data de emissão do Termo de Recebimento Definitivo pela STI/SEF/MG.

14.2.3. A garantia contra defeitos de fabricação, para o item único do lote 2 será de 48 (quarenta e oito) meses, contados a partir da data de emissão do Termo de Recebimento Definitivo pela STI/SEF/MG.

14.2.4. Quando os produtos tiverem prazos de garantia/validade superiores ao mínimo estabelecido, serão estes os considerados.

15. DA SUBCONTRATAÇÃO:

15.1. Caso a CONTRATADA não possua em seu quadro de pessoal profissional(ais) com a capacitação exigida, a execução dos serviços de instalação, configuração, testes em produção e ajustes dos equipamentos/produtos, treinamento, atualização e suporte técnico (subscrição) para a solução de *Firewall,* Lote 1, e garantia e suporte técnico, para o Lote 2, desta contratação, poderá ter como responsável técnico, profissional(ais) do próprio fabricante da solução, mediante subcontratação pelo licitante e sem ônus adicionais para a CONTRATANTE.

15.2. Na hipótese da subcontratação, fica facultado à CONTRANTE exigir da CONTRATADA, a qualquer tempo, durante a vigência do contrato, a apresentação de declaração do fabricante que ateste a sua disponibilidade para a respectiva prestação. No caso de ser a CONTRATADA o responsável técnico, esse deverá comprovar que possui autorização (em vigência) do fabricante para a prestação dos serviços. Tal exigência se justifica tendo em vista a criticidade da solução.

15.3. Vale salientar que esta equipe técnica entende que não é possível tecnicamente a prestação satisfatória dos serviços sem que o fornecedor seja autorizado pelo fabricante. De fato, a responsabilidade técnica é, na prática, sempre do fabricante, uma vez que é ele quem desenvolve o *software* e o *hardware* e seus componentes. Ademais, a Lei de *Software* nº 9.609 de 19 de fevereiro de 1998, garante proteção à propriedade intelectual de programa de computador pela legislação de direitos autorais, sendo ressalvado o direito de o autor opor-se a alterações não-autorizadas, quando essas impliquem deformação, mutilação ou outra modificação do programa de computador, que prejudiquem a sua honra ou a sua reputação. Por essa razão, as alterações em componentes e programas de computador são usualmente realizadas apenas pelo detentor de seus direitos autorais; no caso em questão, trata-se dos fabricantes da solução.

15.4. Vale salientar, no entanto, que os produtos ora contratados poderão ser comercializados por revendedores do fabricante, por essa razão, torna-se necessária a previsão de subcontratação do fabricante como responsável técnico, caso não seja esse o vencedor do certame.

15.5. A subcontratação não eximirá a CONTRATADA das obrigações contratuais e legais, nos termos do art. 72 da Lei Federal nº 8.666/1993.

16. OBRIGAÇÕES ESPECÍFICAS DAS PARTES:

16.1. Da CONTRATADA:

16.1.1. Fornecer os produtos nas quantidades, prazos e condições pactuadas, de acordo com as exigências constantes neste documento.

16.1.2. Emitir faturas no valor pactuado, apresentando-as à CONTRATANTE para ateste e pagamento.

16.1.3. Atender prontamente às orientações e exigências inerentes à execução do objeto contratado.

16.1.4. Reparar, remover, refazer ou substituir, as suas expensas, no todo ou em parte, os itens em que se verificarem defeitos ou incorreções resultantes da execução do objeto, no prazo máximo de 72 (setenta e duas) horas.

16.1.5. Assegurar à CONTRATANTE o direito de sustar, recusar, mandar desfazer ou refazer qualquer serviço/produto que não esteja de acordo com as normas e especificações técnicas recomendadas neste documento.

16.1.6. Assumir inteira responsabilidade pela entrega dos materiais, responsabilizando-se pelo transporte, acondicionamento e descarregamento dos materiais.

16.1.7. Responsabilizar-se pela garantia dos materiais empregados nos itens solicitados, dentro dos padrões adequados de qualidade, segurança, durabilidade e desempenho, conforme previsto na legislação em vigor e na forma exigida neste termo de referência.

16.1.8. Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do objeto deste Termo de Referência.

16.1.9. Não transferir para a CONTRATANTE a responsabilidade pelo pagamento dos encargos estabelecidos no item anterior, quando houver inadimplência da CONTRATADA, nem onerar o objeto deste Termo de Referência.

16.1.10. Manter, durante toda a execução do objeto, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

16.1.11. Manter preposto, aceito pela Administração, para representá-lo na execução do objeto contratado.

16.1.12. Responder pelos danos causados diretamente à CONTRATANTE ou aos seus bens, ou ainda a terceiros, decorrentes de sua culpa ou dolo na execução do objeto;

16.1.13. Devolver na devida proporção, o valor antecipado atualizado caso não executados os serviços contratados, sem prejuízo de multa e demais sanções previstas em lei.

16.2. Da CONTRATANTE:

16.2.1. Acompanhar e fiscalizar os serviços, atestar nas notas fiscais/faturas o efetivo fornecimento do objeto deste Termo de Referência.

16.2.2. Rejeitar, no todo ou em parte os itens entregues, se estiverem em desacordo com a especificação e da proposta de preços da CONTRATADA.

16.2.3. Comunicar a CONTRATADA todas as irregularidades observadas durante o recebimento dos itens solicitados.

16.2.4. Notificar a CONTRATADA no caso de irregularidades encontradas na entrega dos itens solicitados.

16.2.5. Solicitar o reparo, a correção, a remoção ou a substituição dos materiais/serviços em que se verificarem vícios, defeitos ou incorreções.

16.2.6. Conceder prazo de 03 (três) dias úteis, após a notificação, para a CONTRATADA regularizar as falhas observadas.

16.2.7. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA.

16.2.8. Aplicar à CONTRATADA as sanções regulamentares.

16.2.9. Exigir o cumprimento dos recolhimentos tributários, trabalhistas e previdenciários através dos documentos pertinentes.

16.2.10. Disponibilizar local adequado para a realização do serviço.

17. SANÇÕES ADMINISTRATIVAS:

17.1. A CONTRATADA que cometer qualquer das infrações, previstas na Lei Federal nº 8.666, de 21 de junho de 1993, na Lei Federal nº 10.520, de 17 de julho de 2002, Lei Estadual n.º 14.167, de 10 de janeiro de 2002 e no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, E no Decreto Estadual nº 48.012, de 22 de julho de 2020, ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

17.1.1. advertência por escrito;

17.1.2. multa de até:

17.1.2.1. 0,3% (três décimos por cento) por dia, até o trigésimo dia de atraso, sobre o valor do objeto não executado;

17.1.2.2. 10% (dez por cento) sobre o valor da nota de empenho ou do valor total do item 2 do Lote 1, em caso de recusa do adjudicatário em efetuar o reforço de garantia de execução exigida;

17.1.2.3. 20% (vinte por cento) sobre o valor do fornecimento após ultrapassado o prazo de 30 dias de atraso, ou no caso de não entrega do objeto, ou entrega com vícios ou defeitos ocultos que o torne impróprio ao uso a que é destinado, ou diminua-lhe o valor ou, ainda fora das especificações contratadas ;

17.1.2.4. 2% (dois por cento) sobre o valor total do contrato, em caso de descumprimento das demais obrigações contratuais ou norma da legislação pertinente.

17.1.3. Suspensão do direito de participar de licitações e impedimento de contratar com a Administração, pelo prazo de até 2 (dois) anos;

17.1.4. Impedimento de licitar e contratar com a Administração Pública Estadual, nos termos do art. 7º da lei 10.520, de 2002;

17.1.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública;

17.2. A sanção de multa poderá ser aplicada cumulativamente às demais sanções previstas nos itens 17.1.1, 17.1.3, 17.1.4, 17.1.5.

17.3. A multa será descontada da garantia do contrato, quando houver, e/ou de pagamentos eventualmente devidos pelo INFRATOR e/ou cobrada administrativa e/ou judicialmente.

17.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo incidental apensado ao processo licitatório ou ao processo de execução contratual originário que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, bem como o disposto na Lei 8.666, de 1993 e Lei Estadual nº 14.184, de 2002.

17.5. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

17.5.1. Não serão aplicadas sanções administrativas na ocorrência de casos fortuitos, força maior ou razões de interesse público, devidamente comprovados.

17.6. A aplicação de sanções administrativas não reduz nem isenta a obrigação da CONTRATADA de indenizar integralmente eventuais danos causados a Administração ou a terceiros, que poderão ser apurados no mesmo processo administrativo sancionatório.

17.7. As sanções relacionadas nos itens 17.1.3, 17.1.4 e 17.1.5 serão obrigatoriamente registradas no Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual – CAFIMP e no Cadastro Geral de Fornecedores no âmbito da administração direta, autárquica e fundacional do Poder Executivo de Minas Gerais - CAGEF.

17.8. As sanções de suspensão do direito de participar em licitações e impedimento de licitar e contratar com a Administração Pública poderão ser também aplicadas àqueles que:

17.8.1. Retardarem a execução do objeto;

17.8.2. Comportar-se de modo inidôneo;

17.8.2.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

17.8.3. Apresentarem documentação falsa ou cometerem fraude fiscal.

17.9. Durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei Federal nº 12.846, de 2013, e pelo Decreto Estadual nº 46.782, de 2015, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à Controladoria-Geral do Estado, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

18. TERMO DE SIGILO/CONFIDENCIALIDADE:

Juntamente com o contrato de fornecimento deverá ser assinado Termo de Sigilo e Confidencialidade padrão da SEF/MG. O Termo de Confidencialidade é necessário por questão de segurança do negócio da SEF/MG. As informações originadas e tramitadas na prestação de serviços de comunicação do presente objeto são, em quase sua totalidade, sigilosas, portanto, faz-se imprescindível a previsão de celebração de Termo de Confidencialidade neste processo.

19. ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS:

O custo estimado da contratação será tornado público apenas e imediatamente após o encerramento do envio de lances (art. 7º, § 3º, da Lei Federal nº 12.527/2014)", tendo em vista o art. 15, § 1º, do Decreto Estadual nº 48.012/2020: *§ 1º – O caráter sigiloso do valor estimado ou do valor máximo aceitável para a contratação será fundamentado no § 3º do art. 7º da Lei Federal nº 12.527, de 18 de novembro de 2011.*

LINDENBERG NAFFAH FERREIRA
Superintendente de Tecnologia da Informação - STI/SEF

Documento assinado eletronicamente por **Lindenberg Naffah Ferreira**, **Superintendente**, em 22/09/2021, às 20:29, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **34217546** e o código CRC **C3153384**.

Referência: Processo nº 1190.01.0010082/2021-93 SEI nº 34217546

Anexo nº II - Planilha de Especificações/SEF/SPGF-DAC-AQUISIÇÕES/2021

PROCESSO Nº 1190.01.0010082/2021-93

ANEXO II

PLANILHA DE ESPECIFICAÇÕES

LOTE 1 - ITEM 1 – SOLUÇÃO DE SEGURANÇA COM FUNCIONALIDADES DE *FIREWALL*, SISTEMA DE PREVENÇÃO DE INTRUSÃO (IPS), REDES VIRTUAIS PRIVADAS (VPN), CONTROLE DE APLICAÇÕES E AMEAÇAS, FILTRO DE URL E PROTOCOLO DE QUALIDADE DE SERVIÇO (QOS) INTEGRADOS

Subitem		Especificação	Exigência	Ofertado
Descrição	1.0	Solução de segurança com as funcionalidades de *Firewall*, IPS, VPN, Controle de Aplicações, Filtro de URL, *Anti-Malware, Anti-Ransoware,* Anti-Virus para controle de ameaças conhecidas e desconhecidas, em alta disponibilidade composta por *software* para *hardware open server*, *software* de gerenciamento, e demais recursos de acordo com as características técnicas e requisitos gerais relacionados neste documento.	Obrigatório	
	1.1	A solução deverá ser instalada em ambiente de alta disponibilidade com no mínimo 2 (dois) servidores físicos para o ambiente interno e 2 (dois) servidores físicos para o ambiente externo, fornecidos pela CONTRATANTE, com as características especificadas para item único do lote 2 deste Termo de Referência.	Obrigatório	
	1.2	Deverá ser fornecido todo licenciamento de *software* necessário, de forma que a solução a ser fornecida esteja operacional de acordo com as características técnicas e requisitos gerais relacionados neste documento incluindo sistemas operacionais e *hypervisor* de virtualização, caso necessário.	Obrigatório	
		Será aceita atualização do ambiente atual, composto por:		

	1.3	• 2 *appliance* em *cluster* externo Check Point 21400; • 2 *appliance* em *cluster* interno Check Point 21400; • Com *Firewall*, IPSec VPN, IPS, *Application Control, Mobile Acess;* • 2 Servidores em *cluster* virtualizados para gerência da solução, licenciado para até 10 *gateways*. De acordo com as características técnicas e requisitos gerais relacionados neste documento.	Opcional	
Capacidade	2.0	NGFW (*Next Generation Firewall*) de no mínimo 16 Gbps (dezesseis gigabits por segundo), independentemente do tamanho do pacote.	Mínimo Obrigatório	
	2.1	*Threat Protection* de no mínimo 8 Gbps (oito gigabits por segundo).	Mínimo Obrigatório	
	2.2	SSL *Inspection* de no mínimo 6 Gbps (seis gigabits por segundo).	Mínimo Obrigatório	
	2.3	IPsec VPN de no mínimo 14 Gbps (quatorze gigabits por segundo).	Mínimo Obrigatório	
	2.4	Capacidade para suportar no mínimo um *throughput* de 8 Gbps (oito gigabits por segundo) de tráfego inspecionado para *Firewall* considerando todas as funcionalidades habilitadas.	Mínimo obrigatório	
	2.5	Capacidade de 16 Gbps (dezesseis gigabits por segundo) de NGFW para o perfil recomendado pelo fabricante.	Mínimo obrigatório	
	2.6	Permitir 150.000 (cento e cinquenta mil) conexões por segundo (CPS).	Mínimo obrigatório	
	2.7	Permitir 10.000.000 (dez milhões) conexões simultâneas.	Mínimo obrigatório	
	2.8	Capacidade para suportar *throughput* de 7 Gbps (sete gigabits por segundo) de VPN considerando o algoritmo AES-128.	Mínimo obrigatório	
	3.0	Sistema de segurança que provê a capacidade de detecção e bloqueio de ataques sofisticados bem como o reforço granular de políticas de segurança no nível de camada 7 do modelo OSI (aplicação), e atuação como uma plataforma para inspeção do tráfego da rede.	Obrigatório	

Sistema de Segurança	3.1	VPN IPSec e SSL, IPS, controle de aplicações, filtragem de conteúdo e gerenciamento da largura de banda integrados (QoS), sem limitação de usuários e ativos, com atualização de todos os componentes (*engines*, assinaturas, etc.) pelo período da garantia.	Obrigatório	
	3.2	O sistema deve permitir a aplicação de novas configurações de segurança sem interrupção das operações da rede.	Obrigatório	
	3.3	O sistema deve possuir administração unificada da solução, implementada em *hardware* separado e comunicação criptografada entre seus elementos que compõe a solução.	Obrigatório	
	3.4	Permitir a configuração de novas funcionalidades (Vazamento de informações (DLP), IPS, VPN, Antivírus, Filtro de Conteúdo, etc.) sem a necessidade de troca do *hardware* ou reinstalação do *software*.	Obrigatório	
	3.5	Todas as funcionalidades de *firewall* deverão ser fornecidas pelo mesmo fabricante de maneira integrada e em uma mesma arquitetura. Devem ainda ter todas as licenças que compõem a solução ativas e válidas de forma perene, mesmo após o término do contrato, exceto para funcionalidades que dependam de atualizações constantes.	Obrigatório	
	3.6	Os *logs* e objetos devem estar indexados de forma que permitam a rápida busca das informações usando o padrão *Google-Like.*	Obrigatório	
	4.0	A solução deve possibilitar a implementação da tecnologia *Stateful Inspection* que se baseia em análise granular de informações de estado de comunicação e aplicação para conceder o controle de acesso apropriado.	Obrigatório	
	4.1	Ter visibilidade das aplicações e aplicar políticas de segurança na camada de aplicação independente de porta ou protocolo.	Obrigatório	
	4.2	Deve suportar a criação de regras por geolocalização, tanto na origem, quanto no destino, permitindo que o trafego de determinado País/Países sejam bloqueados ou permitidos.	Obrigatório	
	4.3	Deve possibilitar a visualização dos países de origem e destino nos *logs* dos acessos.	Obrigatório	
	4.4	A solução de *firewall* deverá suportar o método de identificação e autenticação por usuário.	Obrigatório	

4.5	Capacidade para autenticar sessões para qualquer serviço, isto é qualquer protocolo e/ou aplicação que façam uso dos protocolos TCP/UDP/ICMP.	Obrigatório	
4.6	A solução de *firewall* deverá ser licenciada para usuários e endereços IPs ilimitados.	Obrigatório	
4.7	A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7, oferecendo controle de acesso com suporte a mais de 3.500 (três mil e quinhentas) aplicações, serviços e protocolos pré-definidos.	Obrigatório	
4.8	Promover a integração com o *Microsoft Active Directory* para a autenticação de usuários, de modo que a solução de *firewall* possa integrar as informações de perfil de usuários armazenadas no serviço de diretórios para realizar a autenticação.	Obrigatório	
4.9	Promover a integração com o protocolo SAML para a autenticação de usuários, pode esse se integrarem com provedor de autenticação em nuvem, como *Azure AD*, *Google Account*, OKTA, de modo que a solução de *firewall* possa integrar as informações de perfil de usuários armazenadas no serviço de diretórios para realizar a autenticação.	Obrigatório	
4.10	Promover a integração com o *Microsoft Active Directory* para identificação transparente de usuários sem necessidade de autenticação direta no *firewall* e implementar políticas de segurança e controle baseadas nestas informações.	Obrigatório	
4.11	Suportar os esquemas de autenticação de usuários tanto para a solução de *firewall* quanto para VPNs como *tokens* (exemplo *SecureID*), TACACS, RADIUS, senha do sistema operacional, senha do próprio *firewall* e *Microsoft Active Directory*, certificados digitais e dispositivos biométricos.	Obrigatório	
4.12	Deve permitir através de configuração que no momento da aplicação da politica de segurança as sessões tenham que ser reestabelecidas.	Obrigatório	
4.13	Deve permitir através de configuração que no momento da aplicação da politica de segurança as sessões sejam mantidas.	Obrigatório	
	Prover mecanismo contra ataques de falsificação de		

	4.14	endereços (IP *Spoofing*) através da especificação da interface de rede pela qual uma comunicação deve se originar.	Obrigatório	
	4.15	Suportar controle de aplicações multimídia, tais como voz sobre IP, áudio e vídeo *streaming*.	Obrigatório	
Firewall	4.16	Capacidade de fazer NAT estático e dinâmico, configurável de forma automática (especificando apenas IP origem e IP traduzido).	Obrigatório	
	4.17	Capacidade de realizar NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional, possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta.	Obrigatório	
	4.18	Permitir a inspeção de tráfego HTTPS (*inbound/outbound*).	Obrigatório	
	4.19	Proteção e suporte às tecnologias de Voz sobre IP SIP e H.323.	Obrigatório	
	4.20	Suportar H.323 V2, 3 e 4.	Obrigatório	
	4.21	Suportar H.225 v2, 3 e 4.	Obrigatório	
	4.22	Suportar H.245 v3, 5 e 7.	Obrigatório	
	4.23	Suportar NAT para H.323 (tecnologia de Voz sobre IP).	Obrigatório	
	4.24	Oferecer proteção para seguintes protocolos de VoIP: MGCP e SCCP (*Skinny Client Control Protocol*).	Obrigatório	
	4.25	Capacidade para suportar IPv6.	Obrigatório	
	4.26	Capacidade de suportar simultaneamente a criação de regras IPv4 e IPv6.	Obrigatório	
	4.27	Capacidade de suportar roteamento estático de tráfego Ipv4 e IPv6.	Obrigatório	
	4.28	Deve suportar a definição de VLAN no *firewall* conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) *interfaces* ou *subinterfaces* lógicas associadas a VLANs e estabelecer regras de filtragem (*Stateful Firewall*) entre elas. O ID das vlans deve ser de 1 a	Obrigatório	

		4090.		
	4.29	Deve possuir suporte a agregação de *links* 802.3ad (LACP).	Obrigatório	
	4.30	Capacidade de suportar SNMP v2 e v3.	Obrigatório	
	4.31	Capacidade de integração com MIBs que possam ser compiladas para o sistema de gerenciamento SNMP.	Obrigatório	
	4.32	Possibilitar o acesso via CLI(Console), SSH, interface Web HTTPS e REST API para configuração e administração local do *Firewall*.	Obrigatório	
	4.33	Possibilitar o acesso via REST API, para executar configurações nas p*olicies* de *Firewall* e de controle de ameaças.	Obrigatório	
	4.34	Deve permitir a criação de rotas estáticas e suportar, no mínimo, os protocolos de roteamento dinâmico OSPFv2, OSPFv3, BGP e RIP.	Obrigatório	
	4.35	Deve possibilitar que as regras de filtragem tenham a capacidade de implementação de CIDR/VLSM.	Obrigatório	
	4.36	Possibilitar a atuação como cliente NTP (*Network Time Protocol*).	Obrigatório	
	4.37	Deve oferecer as funcionalidades de *backup/restore* e deve permitir ao administrador agendar *backups* da configuração em determinado dia e hora.	Obrigatório	
	4.38	Os *backups* devem ficar armazenados localmente e deve existir a funcionalidade de transferi-los a um servidor externo via FTP ou SCP.	Obrigatório	
	5.0	A solução deve prover a possibilidade de criação de políticas integradas para controle de navegação via navegador e controle de aplicações que utilizem ou não o navegador.	Obrigatório	
	5.1	Deve possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.	Obrigatório	
	5.2	Deve identificar, permitir ou bloquear aplicações e páginas da Internet, sem a necessidade de liberação/bloqueio de	Obrigatório	

	portas e protocolos.			
5.3	Deve possuir uma base de aplicações incluindo aplicações, "*Widgets*" Web 2.0 e base de URL.	Obrigatório		
5.4	Deve prover a possibilidade de integrar as funções de controle de aplicações e controle de URL's no mesmo equipamento, sem impossibilitar a ativação de outras funcionalidades de segurança, tais como: • IPS; • Antivírus; • Controle de vazamento de informações.	Obrigatório		
5.5	A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser centralizada na mesma gerência.	Obrigatório		
5.6	A solução deve possibilitar a criação de políticas granulares para as funcionalidades de controle de aplicação e filtro.	Obrigatório		
5.7	Deve possibilitar permitir ou bloquear aplicações ou páginas da Internet por: • Aplicação; • URL; • Aplicação e URL; • Categorias; • Nível de risco; • Endereço IP; • Range de IP's; • Usuários; • Grupos de usuários.	Obrigatório		
5.8	Deve possibilitar a integração da solução com base externa do *Microsoft Active Directory* e LDAP, para criação de políticas, possibilitando a criação de regras utilizando: • Usuários; • Grupo de usuários; • Máquinas (estações de trabalho);	Obrigatório		

		• Endereço IP; • Endereço de Rede; • Combinação das opções acima.		
Controle de Aplicações e Filtragem de Conteúdo.	5.9	Deve prover repositório para consulta em tempo real para URL's e aplicações não categorizadas.	Obrigatório	
	5.10	Deve prover serviço de classificação baseado em "nuvem" (*Cloud based*) para categorização dinâmica do tráfego *Web*.	Obrigatório	
	5.11	Deve possibilitar a customização de aplicações, páginas da Internet, categorias e grupos que não estão na base de aplicações e URL, para utilização na criação de políticas.	Obrigatório	
	5.12	Deve possibilitar a utilização de no mínimo 4 ações nas regras de controle: • Bloquear; • Monitorar; • Informar o usuário; • Interagir com o usuário para decisão da ação (Permitir/Bloquear) possibilitando que o usuário utilize uma justificativa para tal utilização.	Obrigatório	
	5.13	Deve possibilitar a customização, por regra, da tela de interação com o usuário.	Obrigatório	
	5.14	Deve permitir diferentes "telas" de interação com o usuário para equipamentos móveis.	Obrigatório	
	5.15	Deve possibilitar que ações com interações dos usuários sejam aprendidas e utilizadas para eventos similares do mesmo usuário.	Obrigatório	
	5.16	Deve prover agente na estação do usuário para interação com o usuário quando não for possível via navegador.	Obrigatório	
	5.17	Deve permitir a configuração na própria regra limite de utilização de banda tanto para tráfego de "*download*" quanto para "*upload*".	Obrigatório	
	5.18	A solução deve ser capaz de inspecionar o trafego a fim de buscar aplicações que possam comprometer a segurança da CONTRATANTE, como P2P (KaZaa, Gnutella,	Obrigatório	

		Morpheus, BitTorrent, µTorrent) e Ims (Yahoo!, MSN/Skype, ICQ), mesmo quando elas pareçam ser tráfego válido.		
	5.19	Deve oferecer proteção contra *MSN Messenger* / Skype via MSNMS e SIP.	Obrigatório	
	5.20	O administrador deve ser capaz de funcionalidades específicas de páginas Web 2.0 ou aplicações. Por exemplo: bloquear o *chat* e a visualização de vídeos no *Facebook*; bloquear somente a transferência de arquivos no MSN, etc.	Obrigatório	
	5.21	O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos.	Obrigatório	
	5.22	O administrador deve ser capaz de configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.	Obrigatório	
	5.23	Deve oferecer a opção de bloquear controles *ActiveX* e *applets* Java que possam comprometer usuários *web.*	Obrigatório	
	5.24	A solução deve permitir a inspeção de tráfego sobre o protocolo HTTPS (*Inbound/outbound*).	Obrigatório	
	6.0	A solução de Segurança deve ter uma solução de VPN integrada (compartilhar o mesmo *hardware*) para que se possa adicionar e suportar o ambiente de VPN.	Obrigatório	
	6.1	O *software* de VPN e *firewall* devem compartilhar o mesmo *hardware* e sistema operacional, e também os recursos de *cluster*.	Obrigatório	
	6.2	A funcionalidade de IPSec / VPN de todo o *hardware* ofertado deve ser a mesma e deve ser licenciada para funcionamento em *cluster* ativo-ativo e *cluster* ativo-passivo.	Obrigatório	
	6.3	Deve permitir habilitar e desabilitar túneis de VPN a partir da interface gráfica da solução, facilitando o processo de *throubleshooting*.	Obrigatório	
	6.4	Deve ser fornecida licenciamento para criação de no mínimo 8.000 (oito mil) VPN do tipo *site-to-site*.	Obrigatório	

	6.5	Deve suportar o conceito de “comunidades de VPN” (comunidade de *gateways* VPN que se comunicam através de túneis criptografados) permitindo uma configuração centralizada e simplificada dos vários dispositivos de VPN (*gateways*) participantes de tal comunidade, evitando que a configuração seja feita em cada um destes dispositivos por vez.	Obrigatório	
	6.6	Deve suportar esquemas de VPN *site-to-site* em topologias “*Full Meshed*” (cada *gateway* tem um *link* específico para os demais *gateways*), “*Star*” (*gateways* satélites se comunicam somente com o *gateway* central), “*Hub and Spoke*” (onde o *gateway* definido como Hub tem por responsabilidade redirecionar o tráfego para o seu *gateway* destino (*spoke*).	Obrigatório	
	6.7	Deve incluir suporte a *client-to-site* baseado em IPSEC. (mínimo 5.000 usuários simultâneos).	Mínimo Obrigatório	
	6.8	Permitir suporte integrado à VPN SSL client-to-site nativo ou via licenciamento adequado incluso. (mínimo 2.500 usuários simultâneos através de browser).	Mínimo Obrigatório	
	6.9	Suportar os seguintes algoritmos de criptografia simétricos: AES256, AES128, DES, 3DES para fases I e II, assegurando que somente os *peers* que fazem parte da VPN tenham capacidade de entender a mensagem final.	Obrigatório	
	6.10	Permitir que os *gateways* VPN (em uma topologia *site-to-site*) se autentiquem via *preshared secret* e/ou certificados digitais.	Obrigatório	
	6.11	Suportar *Main Mode e Aggressive mode* em IKE *Phase* I.	Obrigatório	
	6.12	Deve suportar integridade de dados MD5 e SHA1.	Obrigatório	
	6.13	Suportar conexões VPN *Client to Site* a partir de aplicativos disponíveis no Microsoft Market.	Obrigatório	
	6.14	Suportar conexões VPN advindas de *clients* L2TP/IPSec nativos em plataformas *Windows* 7, 8, 10 e *Windows Server* 2008 e superiores.	Mínimo Obrigatório	
	6.15	Suportar os algoritmos para geração de chave publica: RSA e *DiffieHellman*, abrangendo os seguintes *groups*: *Group* 1 (768 bits), *Group* 2 (1024 bits), *Group* 5 (1536 bits) e *Group* 14 (2048 bits).	Obrigatório	

VPN	6.16	Suporte para que os clientes VPN possam ter, opcionalmente, camada de *firewall* pessoal (usando o mesmo *software*) para proteção da estação com mecanismos de verificação de configurações desta estação (ex. AntiVirus ativo e atualizado), tendo uma política administrada de forma centralizada pela mesma console de VPN.	Obrigatório	
	6.17	Caso necessite de agentes VPN, o cliente IPSEC VPN incluso deve suportar *roaming* (mudança de redes/interfaces e mudança de endereço IP sem perda da conexão VPN) e *Auto-Connect* (uma conexão é feita automaticamente quando o *endpoint* está fora da rede corporativa e uma aplicação necessita acesso a essa rede).	Obrigatório	
	6.18	Suportar os seguintes esquemas de autenticação de usuários por VPN: usuário e senha em base do próprio sistema de *Firewall*, Serviço de Diretório *Microsoft Active Directory*, certificação digital por meio de certificados emitidos por Autoridade Certificadora no padrão ICP-Brasil.	Obrigatório	
	6.19	Capacidade de otimizar o rendimento de VPN através de técnicas de aceleração por *software*.	Obrigatório	
	6.20	Suportar autoridade certificadora integrada ao *gateway* VPN Autoridade Certificadora integrada à VPN ou a sua console de administrativa como parte nativa da solução, de maneira que se emitam certificados digitais para usuários de VPN e/ou *gateways* de VPN com os quais se estabeleçam comunicação e/ou os componentes da solução (tais como *console* de administração, administradores, módulos, etc.).	Obrigatório	
	6.21	Fácil integração com certificados digitais (PKI) de terceiros, que cumpram com o padrão X.509 para não repúdio de transações por VPN. Pelo menos oferecer a capacidade de integração com 4 diferentes autoridades certificadoras integráveis.	Obrigatório	
	6.22	Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados nos formatos: PKCS#12, CAPI e *Entrust* utilizados no processo de autenticação entre um *gateway* VPN e um usuário remoto (*client-to-site* VPN).	Obrigatório	
	6.23	Suportar a solicitação de emissão de certificados a uma CA *trusted (enrollment*) via SCEP.	Obrigatório	
	6.24	Suporte a algoritmos de compressão de dados, tanto para as VPNs *site-to-site* como para as VPNs *client-to-site*,	Obrigatório	

		realizadas com os clientes próprios.		
	6.25	Oferecer proteção contra ataque IKE DoS, fazendo a distinção entre *peers* conhecidos e desconhecidos.	Obrigatório	
	6.26	Suportar NATT (NAT *Traversal Tunneling*).	Obrigatório	
	6.27	Suportar VPN baseada em rotas, de maneira a conhecer a rota seguinte para envio do tráfego da VPN. Deve suportar ao menos rotas estáticas com opção para suporte à BGP e OSPF como protocolos de roteamento dinâmico para essa característica.	Obrigatório	
	6.28	Clientes IPSec do mesmo fabricante devem estar disponíveis para pelo menos as seguintes plataformas: *GNU/Linux*, *Windows* 7,8, 10 (32bits e 64bits)**,** *Iphone/Ipad* e *Android*.	Mínimo Obrigatório	
	6.29	O acesso VPN SSL deve ser possível para pelo menos as seguintes plataformas: *GNU/Linux*, *Windows* 7,8, 10 (32bits e 64bits)**,** *Iphone/Ipad* e *Android*.	Mínimo Obrigatório	
	6.30	Deve incluir gerenciamento centralizado de VPNs, com a possibilidade de criar várias VPNs ao mesmo tempo.	Obrigatório	
	6.31	Deve permitir que o administrador aplique regras de segurança para controlar o tráfego dentro da VPN	Obrigatório	
	6.32	Deve incluir a funcionalidade para estabelecer VPNs com *gateways* com IPs públicos dinâmicos.	Obrigatório	
	6.33	Deve possuir Portal SSL para acesso às aplicações internas.	Obrigatório	
	6.34	Deve prover acesso via VPN SSL utilizando navegador (*Browser*) sem a necessidade de um cliente instalado na estação. Compatível com os sistemas operacionais Linux, Windows e MacOS.	Obrigatório	
	6.35	Para o acesso via VPN SSL, a solução deverá alocar um endereço IP para estação remota para evitar problemas de roteamento.	Obrigatório	
	7.0	As funcionalidades de IPS e *firewall* devem ser implementadas em um mesmo chassi, sendo que a comunicação entre eles deverá ser interna, sem a necessidade de uso de quaisquer interfaces externas.	Obrigatório	

7.1	Deve incluir pelo menos os seguintes mecanismos de detecção: • Assinaturas de vulnerabilidades e *exploits*; • Assinaturas de ataque; • Validação de protocolo; • Detecção de anomalia; • Detecção baseada em comportamento; • Nível de confiança de detecção de ataque.	Obrigatório	
7.2	O administrador deve ser capaz de configurar a inspeção somente para tráfego entrante (*inbound*).	Obrigatório	
7.3	O IPS deve incluir pelo menos 10.000 (dez mil) definições de ataques que protejam tanto clientes/servidores.	Mínimo Obrigatório	
7.4	O IPS deve oferecer ao menos duas políticas pré-definidas que podem ser usadas imediatamente.	Mínimo Obrigatório	
7.5	As regras de IPS podem ser associadas a um escopo especifico, em que um conjunto especifico de assinaturas estão associadas a um conjunto especifico de objetos de rede.	Obrigatório	
7.6	O IPS deve incluir a habilidade de interromper temporariamente as proteções para fins de *troubleshooting.*	Obrigatório	
7.7	A solução também deve permitir configuração de "*fail-open*" lógico, da função de IPS, em situações que coloquem em risco o funcionamento do *Firewall.*	Obrigatório	
7.8	O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento.	Obrigatório	
7.9	O administrador deve ser capaz de ativar novas proteções baseado em parâmetros configuráveis (impacto no desempenho, severidade da ameaça, proteção dos clientes, proteção dos servidores).	Obrigatório	
7.10	O administrador deve ser capaz de ativar novas proteções baseado em ataques associados a um determinado VENDOR (*Microsoft, Oracle, Siemens*, *etc.*).	Obrigatório	

	7.11	O administrador deve ser capaz de ativar novas proteções baseadas em ataques associados a ataques mais comuns.	Obrigatório	
	7.12	O administrador deve ser capaz de ativar novas proteções baseadas no score do CVE.	Obrigatório	
	7.13	O administrador deve ser capaz de desativar proteções baseadas em ataques obsoletos.	Obrigatório	
	7.14	A solução deve ser capaz de detectar e prevenir as seguintes ameaças: *Exploits* e vulnerabilidades específicas de clientes e servidores, mal uso de protocolos, comunicação *outbound* de *malware*, tentativas de *tunneling*, controle de aplicações, ataques genéricos sem assinaturas pré-definidas.	Obrigatório	
	7.15	Deve oferecer proteções de seguir o uso de aplicações específicas como *peer-to-peer*, com a opção de bloquear estas aplicações.	Obrigatório	
	7.16	Para cada proteção, a descrição da vulnerabilidade e da ameaça, severidade da ameaça e nível de confiança de detecção de ataque devem estar inclusos.	Obrigatório	
	7.17	Para cada escopo de proteção pode se adicionar exceções baseadas em FQDN e País.	Obrigatório	
	7.18	Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na fonte, destino, serviço ou qualquer combinação dos três.	Obrigatório	
	7.19	A solução deve fazer captura de pacotes para proteções específicas.	Obrigatório	
	7.20	A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, redes e VoIP.	Obrigatório	
Controle de Ameaças	7.21	Deve incluir a habilidade de detectar e bloquear ataques conhecidos e desconhecidos, protegendo de, pelo menos, os seguintes ataques conhecidos: IP *Spoofing*, SYN *Flooding*, *Ping of death*, ICMP *Flooding*, *Port Scanning*, ataques de força bruta a IKE e *man-in-the-middle* com VPNs.	Obrigatório	

	7.22	Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades em diversas áreas de interesse do administrador e a evolução no tempo. As diferentes áreas de interesse devem ser definidas usando filtros customizáveis para selecionar alertas baseados em qualquer propriedade ou combinação de propriedades do mesmo, incluindo pelo menos: origem, destino, serviço, tipo e nome do alerta.	Obrigatório	
	7.23	A solução deve permitir a configuração de inspeção do IPS baseado em políticas que utilizem o posicionamento geográfico de origens e destinos do tráfego.	Obrigatório	
	7.24	A solução deve permitir a inspeção de tráfego sobre o protocolo HTTPS (*Inbound/outbound*).	Obrigatório	
	7.25	A solução deve permitir a pré-configuração de no mínimo 10 perfis de proteção de IPS que podem ser utilizados a qualquer momento.	Obrigatório	
	7.26	O sensor do sistema deve impedir *network malware*, incluindo: *Worms* e Virus, *Ransomware*, *Backdoors* e *Trojans*, *Cross-Site Scripting*, SQL *Injections*, *Spyware*, *Phishing*, *Rootkits*, *Anonymizers*, IRC *Bots communications.*	Obrigatório	
	7.27	O sensor do sistema deve impedir comunicação com C&C(*command-and-control*).	Obrigatório	
	7.28	Protocolos de Rede e Serviços de Proteção (RPC, NetBIOS, Telnet, etc).	Obrigatório	
	7.29	O sensor do sistema deve ser capaz de detectar e prevenir ataques baseados em protocolos como *malformed* ICMP *packets* (*Ping of Death*), *source routed pings* (*Land attacks*), etc.	Obrigatório	
	7.30	O sensor do sistema não deve gerar alertas sobre *replays* de ataques *stateless* de assinaturas de ataques válidos que geram grande volumes de *trigges* de falsos ataques capazes de ofuscar o conteúdo do ataque válido.	Obrigatório	
	7.31	O sensor do sistema deve ser capaz de remontar um pacote IP de um ataque de pacote fragmentado antes da aplicação da regra do IPS.	Obrigatório	

	7.32	O sensor do sistema deve ser capaz de realizar inspeção e remontagem de fluxo para evitar técnicas de segmentação TCP, tais como: *interleaved duplicate segments invalid* TCP c*hecksums, segment overlap*, etc.	Obrigatório	
	7.33	O sensor do sistema deve bloquear a atividade da propagação de *malwares* sem bloquear aplicações legítimas, mesmo quando eles são executados no mesmo computador.	Obrigatório	
	7.34	Deve ser possível a implementação em tempo real de bloqueio de trafego suspeito sem a necessidade de mudanças nas regras de acesso.	Obrigatório	
	7.35	Novas assinaturas de IPS podem ser automaticamente instaladas nos gateways assim que disponibilizadas pelo fabricante.	Obrigatório	
	7.36	A solução deve ser capaz de reconstruir arquivos do padrão office (.doc, .xlxs) e PDF em busca de ameaças não conhecidas, paciente de dia zero.	Obrigatório	
	7.37	A solução deve ser capaz de reconstruir arquivos do padrão office (.doc, .xlxs) e entregar ao usuário um cópia em PDF.	Mínino obrigatório	
	7.38	A solução deve ser capaz de realizar emulação de arquivos em busca de anomalias ao acesso da CPU em busca de ameaças não conhecidas.	Obrigatório	
	7.39	A solução deve ser capaz de realizar emulação de arquivos antes que os mesmos sejam entregues ao usuário.	Obrigatório	
	7.40	A solução deve realizar a emulação de arquivos em *Cloud*.	Obrigatório	
	7.41	A solução deve permitir a inspeção de tráfego sobre o protocolo HTTPS (*Inbound/outbound*).	Obrigatório	
	7.42	A solução deve permitir a utilização de no mínimo 4 perfis de proteção contra ameaças preconfiguradas, que permitam a solução adotar as melhores práticas de segurança sem intervenção humana.	Obrigatório	
	8.0	A solução de Segurança deve ter uma solução de *QoS* integrada (compartilhar o mesmo *hardware*) para que se possa adicionar suporte a *QoS*.	Obrigatório	
	8.1	Suportar tecnologia de *QoS* baseada em cotas inteligentes	Obrigatório	

	8.1	para segurança e produtividade.	Obrigatório	
	8.2	Oferecer suporte a *QoS* para tráfego criptografado.	Obrigatório	
	8.3	Suporte a monitoramento gráfico do tráfego que está passando pelo dispositivo em tempo real.	Obrigatório	
	8.4	Capacidade de administração da largura de banda por IP origem, IP destino, direção (de dentro para fora ou de fora para dentro) pelo usuário e horário.	Obrigatório	
	8.5	Capacidade de administração da largura de banda por usuário ou grupo de usuários.	Obrigatório	
QoS	8.6	Suporte a limites (largura de banda máxima a ser utilizada), garantias (mínimo reservado) e pesos relativos (prioridades) como ações para o tráfego classificado.	Obrigatório	
	8.7	Suporte integrado, como parte nativa da solução, a serviços diferenciados (*DiffServ*).	Obrigatório	
	8.8	Permitir que o tráfego marcado (*DiffServ Code Point–DCP*) seja entendido e priorizado inclusive em estruturas de redes MPLS provendo QoS de ponta a ponta.	Obrigatório	
	8.9	Suporte a controles com filas de baixa latência (*Low Latency Queues – LLQ*) para acelerar o tráfego sensível a atraso.	Obrigatório	
	8.10	Suporte à alta disponibilidade transparente, ou seja, sem perda de conexões em texto claro, criptografadas ou classificadas pelo *QoS*, em caso de falha de um dos nós.	Obrigatório	
	8.11	Suporte a balanceamento de carga entre os gateways de *Firewall*/*VPN*/*QoS*.	Obrigatório	
	8.12	Capacidade integrada de *QoS* tanto para tráfego em texto claro como para tráfego *VPN*.	Obrigatório	
	9.0	A solução fornecida deverá ser capaz de suportar a criação de *clusters* com tolerância a falhas, nos modos Alta-Disponibilidade (HA) e/ou cooperativo, em modo ativo-ativo com balanceamento interno.	Obrigatório	
	9.1	A solução deve ser capaz de suportar *cluster* em modo ativo-ativo com no mínimo 2 (dois) membros.	Obrigatório	

Tolerância a Falhas	9.2	No modo Alta-Disponibilidade, a configuração seria a mesma do modo *failover*, porém toda a configuração de estado seria replicada. Desta forma, conexões ativas continuariam funcionando através do *firewall* secundário.	Obrigatório	
	9.3	No modo cooperativo, pelo menos 2 *firewalls* deverão estar em funcionamento simultaneamente, dividindo o tráfego de rede entre eles de forma automática e replicando configuração e estado das conexões também de forma automática.	Obrigatório	
	9.4	No modo cooperativo e alta-disponibilidade, descritos no item anterior, no caso de queda de um dos *firewalls*, não poderá haver perdas das conexões ativas através do *cluster*, mesmo que estas passem por NAT ou VPN.	Obrigatório	
	9.5	Poderão ser aceitos equipamentos adicionais para complementar as funcionalidades de *cluster* exigidas nesta especificação, contando que os itens de desempenho, quantidade de portas e alta disponibilidade sejam cumpridas para cada conjunto de equipamentos e que os equipamentos sejam homologados pelo fabricante do *software* de *firewall.*	Obrigatório	
	10.0	A solução de gerência centralizada das Políticas de Segurança dos *firewalls* deve ser implementada em *hardware* separado.	Obrigatório	
	10.1	A solução de gerência das Políticas deve replicar as alterações para todos os *gateways* envolvidos.	Obrigatório	
	10.2	A especificação do *hardware* necessário para gerência, *logs* e monitoração deve ser fornecida pelo fornecedor, seguindo padrões do fabricante da solução.	Obrigatório	
	10.3	Deverá ser possível a instalação do *software* de gerência em ambiente virtualizado *Vmware*, *MS Hyper-V* e KVM.	Obrigatório	
	10.4	Deve disponibilizar acesso por meio de *browser* ou *client* do próprio fabricante para visualização de políticas, objetos e usuários a fim de prover acesso para gerentes e auditores sem a necessidade de utilizar a console completa.	Obrigatório	
	10.5	O sistema deve prover habilidade de criar regras/politicas de *IPS* para cada interface, virtual interface ou zona de segurança definida.	Obrigatório	

10.6	O sistema de gerencia deve possibilitar o *upgrade* dos *gateways* de segurança através de interface especifica para isso.	Obrigatório	
10.7	O sistema deve suportar upgrade de *software/ruleset* que permitam ao usuário atualizar o *IPS* sem perda de conectividade de rede.	Obrigatório	
10.8	Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de *firewall*, gerência, armazenamento de logs e emissão de relatórios.	Obrigatório	
10.10	Deve oferecer opção de autorizar e bloquear os acessos dos usuários à visualização pelo *browser* ou *client* do próprio fabricante.	Obrigatório	
10.11	O acesso por meio *browser* deve ocorrer sobre SSL.	Obrigatório	
10.12	Deve permitir a criação de regras por intervalo de tempo e/ou período(data e horário de início e fim de validade).	Obrigatório	
10.13	Deve prover, em cada regra, a informação da utilização da mesma. No mínimo: • Percentual de utilização em relação a outras regras; • Número de vezes em que a regra foi utilizada.	Obrigatório	
10.14	Deve suportar que diferentes usuários utilizem a mesma politica no modo de edição ao mesmo tempo.	Obrigatório	
10.15	Deve suportar que o usuário tenha mais de sessão para edição simultaneamente.	Obrigatório	
10.16	Deve permitir a segregação de atividades, em que um usuário possa alterar apenas as funções (por exemplo Controle de Aplicação), mas não possa alterar as configurações de *IPS*.	Obrigatório	
10.17	Deve suportar diferentes perfis de administração, disponibilizando, pelo menos, os seguintes: *read/write, read only*, gerenciamento de usuários e visualização de *logs*.	Obrigatório	
10.18	Deve incluir CA interna x.509 capaz de gerenciar certificados para *gateways* e usuários permitindo autenticação em *VPNs*.	Obrigatório	

	10.19	Deve incluir a capacidade de confiar em CAs externas ilimitadas com a opção de verificar o certificado de cada *gateway* externo através de, no mínimo, DN(*Distinguished Name*) e IP.	Obrigatório	
	10.20	Deve permitir a criação de diversos perfis de IPS a serem aplicados a diferentes *gateways*.	Obrigatório	
	10.21	Deve permitir incorporar automaticamente novas proteções de IPS baseadas, no mínimo, em severidade e nível de confiança da proteção.	Obrigatório	
	10.22	Deve possuir a facilidade de busca com, no mínimo, as opções de consulta: quais objetos contêm IPs específicos ou parte deles, busca por objetos duplicados, busca por objetos não utilizados e listar em quais regras um objeto é utilizado.	Obrigatório	
	10.23	Deve possuir a opção de segmentar as regras de segurança através de rótulos com a finalidade de organizar as políticas.	Obrigatório	
	10.24	Deve prover a opção de salvar automaticamente e manualmente versões de políticas.	Obrigatório	
	10.25	Deve prover a funcionalidade de mover objetos e serviços entre as regras e de uma lista de objetos e serviços para uma regra.	Obrigatório	
	10.26	A solução deverá gerenciar de forma centralizada as licenças dos *gateways* controlados por ela.	Obrigatório	
	10.27	Deve prover a funcionalidade de provisionamento de licenças a partir de um pool de licenças disponível.	Obrigatório	
	10.28	As funcionalidades da solução de armazenamento de logs deverão prover as seguintes características: Deverá possibilitar a filtragem de eventos baseado em diversas categorias (IP origem, porta origem, IP destino, porta destino, interface, categoria de ataque, *translated* IP, *translated port*, entre outras) simultaneamente; Deverá possibilitar a filtragem de eventos relacionados a ação do administrador. No mínimo: • "*login*" e "*logout*"; • Alteração de política;	Obrigatório	

		• Aplicação de alteração de política.		
	10.29	As buscas aos *logs* devem ser *google-like*	Obrigatório	
	10.30	Deverá possibilitar integração com soluções de mercado focadas em correlação de eventos.	Obrigatório	
	10.31	Deverá possibilitar a visualização dos eventos das soluções de segurança na própria solução de gerência.	Obrigatório	
	10.32	Deve incluir um mecanismo automático de captura de pacotes para eventos de IPS com a finalidade facilitar análise forense.	Obrigatório	
	10.33	A solução deverá diferenciar os *logs* para atividades comuns de usuário e *logs* relacionados à gerencia de políticas de segurança.	Obrigatório	
	10.34	A solução deverá permitir configurar para cada tipo de regra ou evento pelo menos três das opções: *log*, alerta, enviar *trap* SNMP, envio de e-mail, execução de *script* definido pelo usuário.	Obrigatório	
	10.35	A solução deverá incluir a opção de alterar uma regra ativa a partir da interface gráfica de visualização de *logs*.	Obrigatório	
	10.36	A solução deve ser capaz de exportar os *logs* para uma base de dados ou repositório externo.	Obrigatório	
Gerência Centralizada do Sistema de Segurança	10.37	A solução deve suportar a troca automática de arquivo de *log*, regularmente ou através do tamanho do arquivo.	Obrigatório	
	10.38	Deve permitir a visualização simultânea de utilização dos recursos do *gateway*. No mínimo: • Utilização de CPU; • Utilização de Memória; • Utilização de disco; • Quantidade de conexões simultâneas; • Quantidade de novas conexões por segundo; • Pacotes bloqueados; • Situação (status) geral das funções de *firewall;* • Situação (status) das funcionalidades de segurança	Obrigatório	

	ativas no *firewall.*		
10.39	Deve permitir a criação de filtros com base em pelo menos as seguintes características do evento: endereço IP de origem e destino, serviço, tipo de evento, severidade do evento e nome do ataque.	Obrigatório	
10.40	Deve permitir ao administrador o agrupamento de eventos baseado em qualquer uma das opções de filtragem, incluindo vários níveis de alinhamento.	Obrigatório	
10.41	Prover mecanismo de visualização de eventos das soluções de segurança, com uma prévia sumarização para fácil visualização de no mínimo as seguintes informações: • Funções de segurança mais utilizadas; • Origem mais utilizada; • Destino mais utilizado; • Regras mais utilizadas; • Usuários com maior atividade.	Obrigatório	
10.42	Deve prover funcionalidades para análise avançada. No mínimo: • Visualizar quantidade de tráfego utilizado de aplicações e navegação; • Gráficos; • Estatísticas.	Obrigatório	
10.43	O administrador deve ser capaz de atribuir filtros para acompanhamento em tempo real, mostrando todos os eventos que corresponda a esse filtro. Permitindo ao operador a concentrar-se sobre os eventos mais importantes.	Obrigatório	
10.44	Deve detectar ataques de negação de serviço e correlacionar eventos de todas as fontes.	Obrigatório	
10.45	Deve suportar a detecção de ataques de força bruta para quebra de credencial.	Obrigatório	
10.46	Deve permitir a geração de relatórios com horários predefinidos, diários, semanais e mensais. Incluindo principais eventos, principais origens, principais destinos, principais Serviços, principais origens e os seus principais eventos, principais destinos e seus principais eventos e	Obrigatório	

	principais serviços e seus principais eventos.		
10.47	Possibilitar o envio de eventos para Sistema de Gerenciamento de Informações de Eventos (SIEM), utilizado pela SEF-MG, HP Arcsight.	Obrigatório	
10.48	Os *logs* podem ser enviados para servidores externos utilizando-se de criptografia TLS.	Obrigatório	
10.49	Possibilitar reação automática para determinados tipos de eventos.	Obrigatório	
10.50	Na função de reação automática deve ser permitida a criação de *"script*".	Obrigatório	
10.51	Deve possibilitar a visualização geográfica dos eventos de segurança.	Obrigatório	
10.52	A ferramenta de relatórios deve fornecer relatórios consolidados e predefinidos sobre: • O volume de conexões que foram bloqueadas pela solução; • Principais fontes de conexões bloqueadas, seus destinos e serviços; • Principais regras usadas pela solução; • Principais ataques detectados pela solução e indicação das suas principais fontes e destinos; • Número de políticas instaladas e desinstaladas na solução; • Principais serviços de rede; • Indicação dos serviços que mais utilizaram tráfego criptografado; • Principais usuários VPN.	Obrigatório	
10.53	A ferramenta de relatórios deve suportar pelo menos os seguintes filtros: endereço de origem, endereço de destino, usuário, nome do ataque e número da regra.	Obrigatório	
10.54	A ferramenta de relatórios deve permitir a personalização de relatórios pré-definidos.	Obrigatório	
10.55	Deve suportar, no mínimo, dois dos seguintes formatos de relatórios: MHT, HTML, PDF, *Microsoft Excel*, *Microsoft*	Obrigatório	

		Visio, ODF e CSV.		
	10.56	Deve suportar a distribuição automática de relatórios por e-mail.	Obrigatório	
	10.57	Deve permitir a integração com nuvens públicas: *Azure, AWS, GCP, Oracle Cloud, Alibaba*.	Obrigatório	
	10.58	Deve permitir a integração com nuvens privadas: *VMWare NSX, Cisco ACI, Openstack e Nuange.*	Obrigatório	
	10.59	A integração com nuvens públicas e privadas deve permitir que uma máquina criada em um desses ambiente receba automaticamente permissão de acesso sem a necessidade de se aplicar uma nova política.	Obrigatório	
	10.60	Deve possuir mecanismo *workflow* para autorização de mudança com perfil de operador, aprovador e gestor.	Obrigatório	
	10.61	Deve possuir ferramenta de verificação de *compliance* para as seguintes regulamentações: SOX, NIST, GDPR, ISO 27001, ISO 27002.	Obrigatório	
	10.62	A atualização da solução de todos os elementos da solução deve ser realizada através da console de gerenciamento.	Obrigatório	
	10.63	A gerência deve permitir versionamento das mudanças realizadas no ambiente.	Obrigatório	
	10.64	A gerência deve permitir retornar o ambiente para uma versão anterior.	Obrigatório	
	10.65	Possibilitar o acesso via CLI (*Console*), SSH, interface Web HTTPS e REST API para configuração e administração local do *Firewall*.	Obrigatório	
	10.66	Possibilitar o acesso via REST API, para executar configurações nas Políticas de *Firewall* e de Controle de Ameaças.	Obrigatório	

LOTE 1 - ITEM 2 - SERVIÇOS DE ATUALIZAÇÃO E SUPORTE TÉCNICO (SUBSCRIÇÃO) PARA A SOLUÇÃO DE *FIREWALL*

Subitem		Especificação	Exigência	Ofertado
		A solução de segurança (Lote1 - item 1) deve possuir		

	1.0	garantia de 12 (doze) meses com um período de disponibilidade para chamada de manutenção de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.	Obrigatório	
	1.1	Os produtos fornecidos no Lote1 - item 1 deverão ter garantia original de fábrica na totalidade de seu funcionamento pelo período mínimo de 12 (doze) meses, contados a partir da data de expedição do Termo de Recebimento Definitivo pela SEF/MG.	Obrigatório	
	1.2	Os chamados de manutenção, dúvidas, entre outros itens abaixo citados, ou até mesmo para contato com o fabricante, serão aberto diretamente pela CONTRATADA para que essa possa intermediar a manutenção, duvidas, entre outros itens abaixo citados. Não deve haver limite para aberturas de chamados, sejam de: • Solução de problemas de configuração e utilização da solução fornecida, inclusive virtualização; • Esclarecimentos de dúvidas sobre a configuração e a utilização dos equipamentos/produtos; • Implementação e customização de novas funcionalidades nos componentes da solução; • Instalação de atualizações de *software* dos produtos fornecidos; • Resolução de problemas na solução ofertada.	Obrigatório	
	1.3	A abertura de chamados poderá ser realizada através de telefone 0800 do fabricante ou parceiro/fornecedor, ou através da página da WEB do fabricante ou parceiro/fornecedor ou através de endereço de e-mail do fabricante ou parceiro/fornecedor.	Obrigatório	
	1.4	A abertura de chamados através de telefone 0800 deverá ser realizada inicialmente em português.	Obrigatório	
		A CONTRATADA deverá realizar os atendimentos, observando a classificação dos problemas reportados e prazo de conclusão do chamado a contar da abertura do chamado técnico de acordo com seu grau de severidade, segundo a seguinte classificação: • **Severidade 1**: problemas que tornem qualquer um dos nós da solução inoperante. **Prazo: 2 (duas) horas,** com atendimento *in-loco*. • **Severidade 2:** problemas ou dúvidas que prejudicam a operação da infraestrutura de rede, mas que não interrompem o acesso aos dados. **Prazo: 8 (oito) horas** com atendimento *in-*		

Suporte, **Garantia e Atualização**	1.5	*loco* ou remoto, a critério da CONTRATADA; • **Severidade 3**: problemas ou dúvidas que criam algumas restrições à operação da infraestrutura. **Prazo: 24 (quarenta e oito) horas** com atendimento *in-loco* ou remoto, a critério da CONTRATADA; • **Severidade 4**: problemas ou dúvidas que não afetam a operação da infraestrutura. **Prazo: 3 (três) dias úteis** com atendimento *in-loco* ou remoto, a critério da CONTRATADA. Entende-se por término do atendimento aos chamados de suporte técnico a disponibilidade do equipamento para uso em perfeitas condições de funcionamento no local onde está instalado.	Obrigatório	
	1.6	Conforme a gravidade ou criticidade do problema a ser resolvido, a CONTRATADA deverá viabilizar o escalonamento do incidente para a área de suporte ou engenharia do fabricante dos produtos devidamente capacitada a resolver o problema, sem custo adicional para a CONTRATANTE.	Obrigatório	
	1.7	A CONTRATADA deverá responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores do quadro da empresa, assim como pelos efeitos delas advindos na execução das atividades previstas nesta especificação técnica ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por estes executadas.	Obrigatório	
	1.8	A CONTRATADA deverá fornecer e aplicar os *patches* de correção, em data e horário a serem definidos pela CONTRATANTE, sempre que forem encontradas falhas de laboratório (*bugs*) ou falhas comprovadas de segurança nos equipamentos/produtos, objeto deste Termo de Referência.	Obrigatório	
	1.9	O serviço de suporte técnico permite o acesso da CONTRATANTE à base de dados de conhecimento do fabricante dos equipamentos/produtos, provendo informações, assistência e orientação para: • Instalação, desinstalação, configuração e atualização de imagem de *software*; • Aplicação de correções (*patches*) de *software*; • Diagnósticos, avaliações e resolução de problemas; características dos equipamentos/produtos e demais atividades relacionadas à correta operação e funcionamento dos mesmos.	Obrigatório	

	1.10	Os *patches* e novas versões de *software* integrante da solução ofertada deverão ser instalados pela CONTRATADA, após aprovação da CONTRATANTE, tão logo estas se tornem disponíveis. A cada atualização realizada deverão ser fornecidos os manuais técnicos originais e documentos comprobatórios do licenciamento da nova versão/*patch.*	Obrigatório	
	1.11	Deverá ser garantido à CONTRATANTE o pleno acesso ao site do fabricante dos equipamentos e *software*. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e *software* especificados, além de permitir *downloads* de quaisquer atualizações de *software* ou documentação deste produto, inclusive base de reputação (subscrição) de todos os itens necessário para total funcionamento da solução.	Obrigatório	
	1.12	Durante o período de suporte técnico, devem ser disponibilizados e instalados, sem ônus à CONTRATANTE, todas as atualizações de *software.*	Obrigatório	

LOTE 2 - ITEM ÚNICO – SERVIDOR PARA SOLUÇÃO DE *FIREWALL*

Lote 2 - Item único – Especificação Servidor para Solução			**Quantidade: 4 unidade**	
Subitem		**Especificação**	**Exigência**	**Ofertado**
Descrição	1.0	Aquisição de servidores para solução de segurança com as características técnicas e requisitos gerais relacionados neste documento.	Obrigatório	
CPU	2.0	02 (dois) Processadores compatíveis com arquitetura *Intel Xeon* de no minimo 3,3GHz (frequência baseada em processador e não em frequência turbo max), 12 núcleos/24 segmentos e observado o desempenho especificado no subitem 11 desta especificação técnica.	Mínimo obrigatório	
	2.1	O processador deverá ser da última geração disponibilizada pelo fabricante no Brasil; O modelo do servidor ofertado deve possuir o índice auditado, no sítio eletrônico oficial SPEC® - http://www.spec.org.	Obrigatório	
	3.0	Suporte para o(s) processador(es) citado(s) no subitem 2.0.	Obrigatório	
	3.1	*Clock* do barramento de sistemas compatível com	Obrigatório	

Placa Mãe	3.1	o *clock* do processador.	Obrigatório	
	3.2	Barramento PCI.	Obrigatório	
	3.3	2 (dois) *slots* de expansão PCIe 3.0.	Obrigatório	
Memoria	4.0	256 GB (4x64 gigabytes ou 8x32 gigabytes) 2933MT/s, *Dual Rank*, BCC.	Mínimo obrigatório	
	4.1	2933MT/s RDIMMs.	Mínimo obrigatório	
Interfaces	5.0	4 portas USB, com pelo menos duas USB 3.0.	Mínimo obrigatório	
	5.1	1 interface serial RS-232.	Mínimo obrigatório	
	5.2	Controladora de vídeo (1 conector VGA).	Mínimo obrigatório	
Armazenamento Interno	6.0	2 (dois) disco SAS com velocidade de rotação 10k ou 15k ou SATA/SAS SSD, com capacidade mínima de 1.000 GB (Um mil gigabytes) cada disco.	Mínimo obrigatório	
	6.1	Controladora RAID PERC H730P, 2GB NV *Cache*, *Minicard.*	Mínimo obrigatório	
Rede	7.0	Placa auxiliar de rede Intel X710 4 portas 10Gbps (SFP+) prontas para uso, DA/SFP+, *Ethernet*. Todos os *transceivers* e SFPs, devem ser fornecidos. As interfaces deverão utilizar driver IXGBE compatível com *multi-queue* de 16 filas.	Obrigatório	
	7.1	2 (duas) portas/*interfaces* 1/10 Gigabit Ethernet 1000Base-T/10GBase-T, padrões IEEE 802.3, full-duplex, *autosensing*, conector RJ-45 fêmea, configuráveis por *software*, *led* indicativo do *status* da conexão.	Mínimo obrigatório	
Software	8.0	Sem sistema operacional.	Obrigatório	
Alimentação	9.0	Fonte de alimentação redundante "*hot swappable*".	Obrigatório	
	9.1	Tensão de 127/220 V e frequência de 60 Hz.	Obrigatório	

Gerência	10.0	Suporte a SNMP.	Obrigatório	
	10.1	Acesso remoto as funções de vídeo, teclado e mouse (KVM) através de interface de gerenciamento Ethernet 10/100 Mbps.	Obrigatório	
Desempenho	11.0	O equipamento ofertado deverá ter desempenho '*SPEC CPU2017 Integer Rate base'*, **mínimo de190 (cento e noventa)**, a ser comprovado através de informações publicadas no *site* www.spec.org ("*All SPEC CPU2017 Results Published by SPEC*" com detalhamento em '*SPEC CPU2017 Integer results'* - http://www.spec.org/cgi-bin/osgresults?conf=rint2017" O índice poderá ser estimado para equipamentos da mesma família para os quais não tenha sido realizado o *benchmark* em questão, mediante utilização de índices de *performance* relativa ou qualquer outra informação que permita correlacionar a capacidade de processamento de equipamentos similares.	Obrigatório	
Característica Física	12.0	Possuir dimensões e acessórios que possibilitem sua fixação em *rack* padrão de 19 polegadas com organizador de cabos.	Obrigatório	
	12.1	O gabinete deverá ter no máximo 1 RU.	Obrigatório	
Certificações	13.0	O equipamento deverá ter aprovação das normas FCC part 15.	Obrigatório	
Documentação	14.0	O equipamento deverá possuir manual (em português ou inglês) de todos os dispositivos e *software* que acompanham o conjunto.	Obrigatório	
	14.1	As informações sobre o atendimento dos requisitos constantes desta especificação técnica deverão estar claramente informadas no catálogo do equipamento publicado pelo fabricante.	Obrigatório	
	14.2	Deverá ser provida toda a documentação técnica que possibilite a averiguação de conformidade com estas especificações. Poderão ser utilizados na proposta da licitante o uso de *datasheets*, manuais e páginas de Internet mantidas pelo fabricante.	Obrigatório	
Acessórios	15.0	Os servidores deverão vir acompanhados dos trilhos para montagem em *rack*, bem como todos os suportes de guia de metal de sustentação dos	Obrigatório	

		cabos de rede e de monitor de vídeo além, dos cabos de alimentação dos servidores.		
	16.0	Todos os componentes integrantes do equipamento devem possuir garantia integral, original de fábrica, contra defeitos de fabricação, por período não inferior a 48 (quarenta e oito) meses contados a partir da data de expedição do Termo de Recebimento Definitivo, sem ônus adicional para a CONTRATANTE.	Mínimo obrigatório	
	16.1	A prestação de serviços de suporte técnico, correção de problemas e atualização de versões (manutenção) relativa aos *software* fornecidos, incluindo para o Sistema Operacional, deve ser pelo período mínimo de 48 (quarenta e oito) meses, sem ônus adicional para a CONTRATANTE.	Mínimo obrigatório	
	16.2	A CONTRATADA deverá identificar, habilitar e manter um canal de contato técnico junto ao fabricante para acesso direto da CONTRATANTE por meio de seus representantes credenciados. Este canal de contato deverá ser configurado para acesso direto a técnicos habilitados do fabricante visando à resolução de problemas e/ou orientação direta aos técnicos da CONTRATANTE.	Mínimo obrigatório	
	16.3	A CONTRATADA deverá fornecer lista com todos os dados necessários para abertura de chamados técnicos (por exemplo: códigos de identificação dos equipamentos, descrição, versão de firmware, etc.).	Obrigatório	
	16.4	O atendimento de suporte técnico deverá ser via “Central de Atendimento ao Usuário” para abertura de chamados e resolução de problemas tipo 24x7 (vinte e quatro horas por dia, sete dias por semana).	Obrigatório	
	16.5	A CONTRATADA deverá substituir todos os componentes (exceto os gabinetes) do equipamento fornecido e já instalado por outros iguais ou superiores, em perfeito estado de funcionamento, no prazo de 60 (sessenta) dias após solicitação da CONTRATANTE, na ocorrência de mais de 4 (quatro) eventos que totalizem 32 (trinta e duas) horas de indisponibilidade e que comprometam o seu perfeito funcionamento dentro de um período contínuo qualquer de 30 (trinta) dias.	Obrigatório	
	16.6	A substituição não acarretará ônus para a CONTRATANTE e não eximirá o fornecedor das penalidades previstas.	Obrigatório	

Garantia	16.7	A assistência técnica utilizará apenas peças e componentes originais, salvo nos casos fundamentados por escrito e aceitos pela CONTRATANTE.	Obrigatório	
	16.8	Para complementar a garantia oferecida pelo fabricante, a CONTRATADA deverá prestar serviço de assistência técnica. Este serviço será prestado durante a vigência da garantia, que é de 48 (quarenta e oito) meses, e garantirá à CONTRATANTE o cumprimento de limites para o prazo de atendimento e de solução do problema exigidos. • O prazo de atendimento para chamados técnicos relativos a eventos de indisponibilidade ou manutenção de *hardware* será do tipo 24x7 (7 dias por semana, 24 horas por dia), com atendimento em até 4 (quatro) horas corridas após o chamado e solução do problema em até 48 (quarenta e oito) horas corridas. O prazo de atendimento é dado pelo tempo decorrido entre a abertura do chamado pela CONTRATANTE e o início da atividade de diagnóstico pela CONTRATADA. A atividade será considerada iniciada a partir da chegada do técnico da CONTRATADA na Superintendência de Tecnologia da Informação ou unidade equivalente da CONTRATANTE, ou a partir do horário do acesso remoto registrado no log do equipamento ou ainda a partir do contato efetuado por telefone pelo técnico da CONTRATADA, a critério da CONTRATANTE. • O prazo de solução para evento de indisponibilidade será contado a partir da abertura do chamado pela CONTRATANTE. • Entende-se como solução do problema: 1. Em caso de defeito de *hardware*, a correção do defeito ou o retorno do acesso aos dados; 2. Em caso de problemas em *software* ou microcódigo, a correção do defeito ou implementação de solução de contorno para o retorno do acesso aos dados, desde que a correção definitiva ocorra posteriormente, dentro de um prazo acordado entre as partes, em função da complexidade da ocorrência.	Obrigatório	
		Ao final de cada atendimento resultante de abertura de chamado, por parte da área de TI da		

	16.9	CONTRATANTE, a CONTRATADA deverá emitir laudo técnico contendo no mínimo: • Data e hora do chamado; • Data e hora do início e do término do atendimento; • Identificação do defeito; • Identificação unívoca do equipamento (componente que apresentou problemas); • Providências adotadas.	Mínimo obrigatório	
	16.10	Atualização de *firmware* de todos os componentes da solução durante todo o prazo de garantia do equipamento, sem custo adicional para a CONTRATANTE.	Obrigatório	
	16.11	Caso o fornecedor entenda necessária a realização de serviços de manutenção preventiva, estes deverão ser agendados com antecedência mínima de 5 (cinco) dias úteis.	Obrigatório	
	16.12	Alterações nas configurações realizadas durante a execução desta assistência técnica deverão ser atualizadas na documentação especificada.	Obrigatório	
	16.13	A manutenção e troca de peças deverão ser executadas por técnicos certificados pelo fabricante, no local onde se encontra o equipamento (*on site*).	Obrigatório	
Suporte técnico	17.0	Deverá ser prestado incondicionalmente, sem custos adicionais, acesso liberado ao sítio na Internet do fabricante, onde seja possível encontrar os seguintes itens de suporte mínimo: • Possibilitar *download* de atualizações de todas as versões de *software* fornecidos; • Possibilitar o acesso a *drivers* de dispositivos, sistemas embarcados – componentes, interfaces de rede, controladoras, etc.; • Novas versões de *software* lançadas durante o período de garantia, possibilitando acesso de forma *on-line* ou efetuar *download* de *software*, manuais ou guias de referência técnicas de componentes dos componentes de *software* necessários ao funcionamento da solução fornecida.	Mínimo obrigatório	

Instalação	18.0	Este serviço consiste na colocação do equipamento em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no edital e seus Anexos, e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da CONTRATANTE.	Obrigatório	
	18.1	A instalação física do equipamento será realizada pelo fornecedor, com acompanhamento de uma equipe destacada pela CONTRATANTE.	Obrigatório	
	18.2	A instalação, configuração e testes do equipamento deverão ser feitos com o acompanhamento de técnicos da CONTRATANTE, visando ao repasse de conhecimento e observados os padrões segurança da CONTRATANTE.	Obrigatório	
	18.3	O equipamento deverá estar com todas as funcionalidades e recursos de *hardware* e *software* solicitados disponíveis e configurados. Os sistemas de gerenciamento e de acionamento automático de suporte técnico também deverão estar ativos e em pleno funcionamento, levando em consideração todas as características solicitadas.	Obrigatório	
	18.4	A instalação e a configuração do equipamento deverão ocorrer preferencialmente em dias úteis, de 9 às 17 horas, ficando a cargo da CONTRATANTE a definição dos horários para configuração do equipamento em produção. Atividades a serem realizadas fora deste horário estarão sujeitas à aprovação prévia da equipe da área de TI da CONTRATANTE.	Obrigatório	
	18.5	Todos os componentes de *hardware* e *software* deverão funcionar em conjunto, simultaneamente, sem conflitos, de forma integrada entre eles e o ambiente de infraestrutura de TI da CONTRATANTE.	Obrigatório	
Capacitação técnica	19.0	Fornecer capacitação dos técnicos da CONTRATANTE no modelo "*hands-on*" para a instalação e configuração do equipamento, provendo os técnicos da área de TI da CONTRATANTE a capacidade de gerenciamento e manutenção da solução em todas as suas funcionalidades, inclusive aquelas não expressamente exigidas como requisitos, mas disponíveis na solução ofertada.	Obrigatório	

LOTE 2 - ITEM ÚNICO – SOLUÇÃO DE SEGURANÇA COM FUNCIONALIDADES DE FIREWALL, SISTEMA DE PREVENÇÃO DE INTRUSÃO (IPS), REDES VIRTUAIS PRIVADAS (VPN), CONTROLE DE APLICAÇÕES E AMEAÇAS, FILTRO DE URL E PROTOCOLO DE QUALIDADE DE SERVIÇO (QOS) INTEGRADOS

Lote 2 - Item único – Especificação Servidor para Solução			**Quantidade: 4 unidade**	**Ofertado**
Subitem		**Especificação**	**Exigência**	
Descrição	1.0	Aquisição de servidores para Solução de segurança com as características técnicas e requisitos gerais relacionados neste documento.	Obrigatório	
CPU	2.0	02 (dois) Processadores compatíveis com arquitetura Intel Xeon de no minimo 3,3GHz (frequência baseada em processador e não em frequência turbo max), 12 núcleos/24 segmentos e observado o desempenho especificado no subitem 10 desta especificação técnica.	Mínimo obrigatório	
	2.1	O processador deverá ser da última geração disponibilizada pelo fabricante no Brasil; O modelo do servidor ofertado deve possuir o índice auditado, no sítio eletrônico oficial SPEC® - http://www.spec.org	Obrigatório	
Placa Mãe	3.0	Suporte para o(s) processador(es) citado(s) no subitem 2.0	Obrigatório	
	3.1	*Clock* do barramento de sistemas compatível com o *clock* do processador	Obrigatório	
	3.2	Barramento PCI	Obrigatório	

	3.3	2 (dois) slots de expansão PCIe 3.0.	Obrigatório	
Memoria	4.0	256 GB (4x64 gigabytes ou 8x32 gigabytes) 2933MT/s, *Dual Rank*, BCC.	Mínimo obrigatório	
	4.1	2933MT/s RDIMMs	Mínimo obrigatório	
Interfaces	5.0	4 portas USB, com pelo menos duas USB 3.0	Mínimo obrigatório	
	5.1	1 interface serial RS-232	Mínimo obrigatório	
	5.2	Controladora de vídeo (1 conector VGA)	Mínimo obrigatório	
Armazenamento Interno	6.0	2 (dois) disco SAS com velocidade de rotação 10k ou 15k ou SATA/SAS SSD, com capacidade mínima de 1.000 GB (Um mil gigabytes) cada disco.	Mínimo obrigatório	
	6.1	Controladora RAID PERC H730P, 2GB NV Cache, *Minicard*	Mínimo obrigatório	
Rede	7.0	Placa auxiliar de rede Intel X710 4 portas 10Gbps (SFP+) prontas para uso, DA/SFP+, Ethernet. Todos os *transceivers* e SFPs, devem ser fornecidos. As interfaces deverão utilizar driver IXGBE compatível com *multi-queue* de 16 filas.	Obrigatório	
	7.1	2 (duas) portas/*interfaces* 1/10 Gigabit Ethernet 1000Base-T/10GBase-T, padrões IEEE 802.3, full-duplex, *autosensing*, conector RJ-45 fêmea, configuráveis por *software*, *led* indicativo do *status* da conexão	Mínimo obrigatório	

Software	8.0	Sem sistema operacional	Obrigatório	
Alimentação	9.0	Fonte de alimentação redundante "*hot swappable*"	Obrigatório	
	9.1	Tensão de 127/220 V e frequência de 60 Hz.	Obrigatório	
Gerência	10.0	Suporte a SNMP	Obrigatório	
	10.1	Acesso remoto as funções de vídeo, teclado e mouse (KVM) através de interface de gerenciamento Ethernet 10/100 Mbps	Obrigatório	
Desempenho	11.0	O equipamento ofertado deverá ter desempenho '*SPEC CPU2017 Integer Rate base*', mínimo de 170 (cento e setenta), a ser comprovado através de informações publicadas no *site* www.spec.org ("All SPEC CPU2017 Results Published by SPEC" com detalhamento em '*SPEC CPU2017 Integer results*' - http://www.spec.org/cgi-bin/osgresults? conf=rint2017" O índice poderá ser estimado para equipamentos da mesma família para os quais não tenha sido realizado o *benchmark* em questão, mediante utilização de índices de *performance* relativa ou qualquer outra informação que permita correlacionar a capacidade de processamento de equipamentos similares.	Obrigatório	
Característica Física	12.0	Possuir dimensões e acessórios que possibilitem sua fixação e m *rack* padrão de 19 polegadas com	Obrigatório	

Física		organizador de cabos.		
	12.1	O gabinete deverá ter no máximo 1 RU´s.	Obrigatório	
Certificações	13.0	O equipamento deverá ter aprovação das normas FCC part 15.	Obrigatório	
Documentação	14.0	O equipamento deverá possuir manual (em português ou inglês) de todos os dispositivos e *software* que acompanham o conjunto.	Obrigatório	
	14.1	As informações sobre o atendimento dos requisitos constantes desta especificação técnica deverão estar claramente informadas no catálogo do equipamento publicado pelo fabricante.	Obrigatório	
	14.2	Deverá ser provida toda a documentação técnica que possibilite a averiguação de conformidade com estas especificações. Poderão ser utilizados na proposta da licitante o uso de *datasheets*, manuais e páginas de Internet mantidas pelo fabricante.	Obrigatório	
Acessórios	15.0	Os servidores deverão vir acompanhados dos trilhos para montagem em *rack*, bem como todos os suportes de guia de metal de sustentação dos cabos de rede e de monitor de vídeo além, dos cabos de alimentação dos servidores.	Obrigatório	
		Todos os componentes integrantes do equipamento devem		

	16.0	possuir garantia integral, original de fábrica, contra defeitos de fabricação, por período não inferior a 48 (quarenta e oito) meses contados a partir da data de expedição do Termo de Recebimento Definitivo, sem ônus adicional para a CONTRATANTE.	Mínimo obrigatório	
	16.1	A prestação de serviços de suporte técnico, correção de problemas e atualização de versões (manutenção) relativa aos software fornecidos, incluindo para o Sistema Operacional, deve ser pelo período mínimo de 48 (quarenta e oito) meses, sem ônus adicional para a CONTRATANTE.	Mínimo obrigatório	
	16.2	A CONTRATADA deverá identificar, habilitar e manter um canal de contato técnico junto ao fabricante para acesso direto da CONTRATANTE por meio de seus representantes credenciados. Este canal de contato deverá ser configurado para acesso direto a técnicos habilitados do fabricante visando à resolução de problemas e/ou orientação direta aos técnicos da CONTRATANTE.	Mínimo obrigatório	
	16.3	A CONTRATADA deverá fornecer lista com todos os dados necessários para abertura de chamados técnicos (por exemplo: códigos de identificação dos equipamentos,	Obrigatório	

		descrição, versão de firmware, etc.).		
	16.4	O atendimento de suporte técnico deverá ser via “Central de Atendimento ao Usuário” para abertura de chamados e resolução de problemas tipo 24x7 (vinte e quatro horas por dia, sete dias por semana).	Obrigatório	
	16.5	A CONTRATADA deverá substituir todos os componentes (exceto os gabinetes) do equipamento fornecido e já instalado por outros iguais ou superiores, em perfeito estado de funcionamento, no prazo de 60 (sessenta) dias após solicitação da CONTRATANTE, na ocorrência de mais de 4 (quatro) eventos que totalizem 32 (trinta e duas) horas de indisponibilidade e que comprometam o seu perfeito funcionamento dentro de um período contínuo qualquer de 30 (trinta) dias.	Obrigatório	
	16.6	A substituição não acarretará ônus para a CONTRATANTE e não eximirá o fornecedor das penalidades previstas.	Obrigatório	
	16.7	A assistência técnica utilizará apenas peças e componentes originais, salvo nos casos fundamentados por escrito e aceitos pela CONTRATANTE.	Obrigatório	
		Para complementar a garantia oferecida pelo fabricante, a		

Garantia	16.8	CONTRATADA deverá prestar serviço de assistência técnica. Este serviço será prestado durante a vigência da garantia, que é de 48 (quarenta e oito) meses, e garantirá à CONTRATANTE o cumprimento de limites para o prazo de atendimento e de solução do problema exigidos. • O prazo de atendimento para chamados técnicos relativos a eventos de indisponibilidade ou manutenção de hardware será do tipo 24x7 (7 dias por semana, 24 horas por dia), com atendimento em até 4 (quatro) horas corridas após o chamado e solução do problema em até 48 (quarenta e oito) horas corridas. O prazo de atendimento é dado pelo tempo decorrido entre a abertura do chamado pela CONTRATANTE e o início da atividade de diagnóstico pela CONTRATADA. A atividade será considerada iniciada a partir da chegada do técnico da CONTRATADA na Superintendência de Tecnologia da Informação ou unidade equivalente da CONTRATANTE, ou a partir do	Obrigatório		

			horário do acesso remoto registrado no log do equipamento ou ainda a partir do contato efetuado por telefone pelo técnico da CONTRATADA, a critério da CONTRATANTE. • O prazo de solução para evento de indisponibilidade será contado a partir da abertura do chamado pela CONTRATANTE. • Entende-se como solução do problema: • Em caso de defeito de *hardware*, a correção do defeito ou o retorno do acesso aos dados; • Em caso de problemas em *software* ou microcódigo, a correção do defeito ou implementação de solução de contorno para o retorno do acesso aos dados, desde que a correção definitiva ocorra posteriormente, dentro de um prazo acordado entre as partes, em função da complexidade da ocorrência.		
			Ao final de cada atendimento resultante de abertura de chamado, por parte da área de TI da CONTRATANTE, a CONTRATADA deverá		

	16.9	emitir laudo técnico contendo no mínimo: • Data e hora do chamado; • Data e hora do início e do término do atendimento; • Identificação do defeito; • Identificação unívoca do equipamento (componente que apresentou problemas) e; • Providências adotadas.	Mínimo obrigatório	
	16.10	Atualização de *firmware* de todos os componentes da solução durante todo o prazo de garantia do equipamento, sem custo adicional para a CONTRATANTE.	Obrigatório	
	16.11	Caso o fornecedor entenda necessária a realização de serviços de manutenção preventiva, estes deverão ser agendados com antecedência mínima de 5 (cinco) dias úteis.	Obrigatório	
	16.12	Alterações nas configurações realizadas durante a execução desta assistência técnica deverão ser atualizadas na documentação especificada	Obrigatório	
	16.13	A manutenção e troca de peças deverão ser executadas por técnicos do fornecedor no local onde se encontra o equipamento (*on site*).	Obrigatório	

Suporte técnico	17.0	Deverá ser prestado incondicionalmente, sem custos adicionais, acesso liberado ao sítio na Internet do fabricante, onde seja possível encontrar os seguintes itens de suporte mínimo: • Possibilitar *download* de atualizações de todas as versões de software fornecidos; • Possibilitar o acesso a *drivers* de dispositivos, sistemas embarcados – componentes, interfaces de rede, controladoras, etc.; • Novas versões de *software* lançadas durante o período de garantia, possibilitando acesso de forma *on-line* ou efetuar *download* de *software*, manuais ou guias de referência técnicas de componentes dos componentes de software necessários ao funcionamento da solução fornecida.	Mínimo obrigatório	
	18.0	Este serviço consiste na colocação do equipamento em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no edital e seus Anexos, e em perfeitas condições de operação, de forma integrada ao ambiente de	Obrigatório	

		infraestrutura de informática da CONTRATANTE.		
	18.1	A instalação física do equipamento será realizada pelo fornecedor, com acompanhamento de uma equipe destacada pela CONTRATANTE.	Obrigatório	
	18.2	A instalação, configuração e testes do equipamento deverão ser feitos com o acompanhamento de técnicos da CONTRATANTE, visando ao repasse de conhecimento e observados os padrões segurança da CONTRATANTE.	Obrigatório	
Instalação	18.3	O equipamento deverá estar com todas as funcionalidades e recursos de *hardware* e *s o f t w a r e* solicitados disponíveis e configurados. Os sistemas de gerenciamento e de acionamento automático de suporte técnico também deverão estar ativos e em pleno funcionamento, levando em consideração todas as características solicitadas.	Obrigatório	
	18.4	A instalação e a configuração do equipamento deverão ocorrer preferencialmente em dias úteis, de 9 às 17 horas, ficando a cargo da CONTRATANTE a definição dos horários para configuração do equipamento em produção. Atividades a	Obrigatório	

		serem realizadas fora deste horário estarão sujeitas à aprovação prévia da equipe da área de TI da CONTRATANTE.		
	18.5	Todos os componentes de *hardware* e *software* deverão funcionar em conjunto, simultaneamente, sem conflitos, de forma integrada entre eles e o ambiente de infraestrutura de TI da CONTRATANTE.	Obrigatório	
Capacitação técnica	19.0	Fornecer capacitação dos técnicos da CONTRATANTE no modelo "*hands-on*" para a instalação e configuração do equipamento, provendo os técnicos da área de TI da CONTRATANTE a capacidade de gerenciamento e manutenção da solução em todas as suas funcionalidades, inclusive aquelas não expressamente exigidas como requisitos, mas disponíveis na solução ofertada.	Obrigatório	

Documento assinado eletronicamente por **Lindenberg Naffah Ferreira**, **Superintendente**, em 22/09/2021, às 20:29, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **34217797** e o código CRC **615A8E07**.

Referência: Processo nº 1190.01.0010082/2021-93 SEI nº 34217797

ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
Diretoria de Aquisições e Contratos/Divisão de Aquisições

Versão v.20.09.2020.

ANEXOS

ANEXO III

MODELO DE PROPOSTA COMERCIAL PARA FORNECIMENTO DE BENS

PROPOSTA COMERCIAL PARA O PREGÃO ELETRÔNICO Nº 1191001 48/2021
(preenchida em papel timbrado da proponente)

DADOS A CONSTAR NA PROPOSTA	PREENCHIMENTO PELO PROPONENTE
Razão Social	
CNPJ	
Endereço	
Telefone	
Endereço Eletrônico	
Nome do Representante Legal	
CPF do Representante Legal	

LOTE 1

Item	Quant.	CodIgo Item SIAD	Descrição do Item	Valor Unitário		Valor Total	
				SEM ICMS	COM ICMS	SEM ICMS	COM ICMS
1	1	107492	Solução de segurança com funcionalidades de *Firewall*, Sistema de Prevenção de Intrusão (IPS), Redes Virtuais Privadas (VPN), Controle de Aplicações e Ameaças, Filtro de URL e Protocolo de Qualidade de Serviço (*QoS*) Integrados				
2	1	107506	Serviços de atualização e suporte técnico (subscrição) para a solução de *Firewall*.				
3	1	107514	Serviços de instalação, configuração, testes em produção e ajustes dos equipamentos/produtos da solução *Firewall*				
4	1	107590	Serviços de treinamento da solução *Firewall*				

VALOR GLOBAL (SOMATÓRIO VALOR TOTAL) LOTE 01 SEM ICMS	**R$ _____ (_____)**
VALOR GLOBAL (SOMATÓRIO VALOR TOTAL) LOTE 01 COM ICMS	**R$** _____ (_____)

LOTE 2

Item	Quant.	CódIgo Item SIAD	Descrição do Item	Valor Unitário		Valor Total	
				SEM ICMS	COM ICMS	SEM ICMS	COM ICMS
único	4	1816470	Servidor para Solução *de Segurança*				

VALOR GLOBAL (SOMATÓRIO VALOR TOTAL) LOTE 02 SEM ICMS	**R$ _____ (_____)**
VALOR GLOBAL (SOMATÓRIO VALOR TOTAL) LOTE 02 COM ICMS	**R$ _____ (_____)**

Prazo de Validade da Proposta:	
Local de Entrega	

Declaro que serão atendidas todas as condições comerciais estabelecidas no Anexo I do Edital.

Declaro que nos preços propostos encontram-se incluídos todos os tributos, encargos sociais, trabalhistas e financeiros, taxas, seguros e quaisquer outros ônus que porventura possam recair sobre o objeto a ser contratado na presente licitação e que estou de acordo com todas as normas da solicitação de propostas e seus anexos.

Declaro que esta proposta foi elaborada de forma independente.

Data e local.

Assinatura do Representante Legal da Empresa

Documento assinado eletronicamente por **Arilson Leandro Fernandes Correa Lopes**, **Diretor**, em 23/09/2021, às 10:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **34217873** e o código CRC **09457512**.

Versão v.20.09.2020.

SEF/SPGF-DAC-AQUISIÇÕES

Belo Horizonte, 24 de agosto de 2021.

ANEXO IV

SUGESTÕES DE MODELOS DE DECLARAÇÕES

(PAPEL TIMBRADO DA EMPRESA)

DECLARAÇÃO DE MENORES

A _____, CNPJ nº. _____, com sede à_____, declara, sob as penas da lei, a inexistência de trabalho noturno, perigoso ou insalubre por menores de 18 (dezoito) anos ou a realização de qualquer trabalho por menores de 16 (dezesseis) anos, salvo menor, a partir dos 14 anos, na condição de aprendiz, nos termos do artigo 7º, inciso XXXIII, da Constituição Federal.

Data e local.

_____

Assinatura do Representante Legal da Empresa

(PAPEL TIMBRADO DA EMPRESA)

DECLARAÇÃO DE CUMPRIMENTO DO PARÁGRAFO ÚNICO DO ART. 13 DE DECRETO ESTADUAL Nº 47.437, de 2018

A _____, CNPJ nº. _____, com sede à_____, declara, sob as penas da lei, que cumpre todos os requisitos legais para sua categorização como _____, estando no

rol descrito no item 4.3 deste edital, não havendo quaisquer impedimentos que a impeça de usufruir do tratamento favorecido diferenciado estabelecido nos arts. 42 a 49 da Lei Complementar nº 123, de 2006, e Decreto Estadual nº 47.437, de 2018.

Data e local.

_____

Assinatura do Representante Legal da Empresa

(PAPEL TIMBRADO DA EMPRESA)

DECLARAÇÃO DE CIÊNCIA DAS CONDIÇÕES DO EDITAL E SEUS ANEXOS

A _____, CNPJ nº. _____, com sede à_____, declara, sob as penas da lei, que está ciente das condições contidas neste edital e seus anexos.

Data e local.

_____

Assinatura do Representante Legal da Empresa

(PAPEL TIMBRADO DA EMPRESA)

DECLARAÇÃO DE AUSÊNCIA DE TRABALHO DEGRADANTE OU FORÇADO

A _____, CNPJ nº. _____, com sede à_____, declara, sob as penas da lei, que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observado o disposto nos incisos III e IV do artigo 1º e no inciso III do artigo 5º da Constituição Federal.

Data e local.

_____

Assinatura do Representante Legal da Empresa

Correa Lopes, **Diretor**, em 23/09/2021, às 10:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **34217964** e o código CRC **9BCF8B09**.

Referência: Processo nº 1190.01.0010082/2021-93 SEI nº 34217964

SECRETARIA DE ESTADO DE FAZENDA

Rodovia Papa João Paulo II, 4001 - Edifício Gerais - Bairro Serra Verde / Belo Horizonte - CEP 31630-901

Versão v.11.08.2021.

Processo nº 1190.01.0010082/2021-93

ANEXO V

TERMO DE CONTRATO

CONTRATO Nº , DE COMPRA, QUE ENTRE SI CELEBRAM O ESTADO DE MINAS GERAIS, POR INTERMÉDIO DA SECRETARIA DE ESTADO DE FAZENDA DE MINAS GERAIS/SUPERINTENDÊNCIA DE DE TECNOLOGIA DA INFORMAÇÃO E A EMPRESA [INSERIR NOME DA EMPRESA], NA FORMA ABAIXO:

O Estado de Minas Gerais, por meio da Secretaria de Estado de Fazenda, com sede na Cidade Administrativa, Rodovia Papa João Paulo II, nº 4.001, Prédio Gerais - 6º andar, Lado Ímpar - Bairro Serra Verde, na cidade de Belo Horizonte/Estado de Minas Gerais, endereço de correio eletrônico: stidgvdce@fazenda.mg.gov.br, inscrita no CNPJ sob o nº 16.907.746/0001-13, doravante denominada **CONTRATANTE**, neste ato representado pelo Sr. Lindenberg Naffah Ferreira, inscrito no CPF sob o nº 571.685.717-53, Resolução de competência nº 3.597 de 03/12/2004 e a empresa [inserir nome da empresa], endereço de correio eletrônico [inserir e-mail], inscrito(a) no Cadastro Nacional da Pessoa Jurídica – CNPJ – sob o número [inserir nº do CNJP], com sede na [inserir nome da cidade sede da empresa], neste ato representada pelo Sr(a). [inserir nome do representante da contratada], inscrito(a) no CPF nº [inserir nº do CPF], doravante denominada **CONTRATADA**, celebram o presente Contrato, decorrente do **Pregão Eletrônico nº 1191001 48/2021**, que será regido pela Lei Federal nº 10.520/2002, Decreto Estadual n° 48.012/2020, e subsidiariamente pela Lei nº 8.666/1993, com suas alterações posteriores, aplicando-se ainda, no que couber, as demais normas específicas aplicáveis ao objeto, ainda que não citadas expressamente.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente Termo de Contrato é a aquisição de *(preencher de acordo com o lote a ser adjudicado)*, conforme especificações e quantitativos estabelecidos no Edital do Pregão nº 1191001 48/2021 identificado no preâmbulo e na proposta vencedora, os quais integram este instrumento, independente de transcrição.

1.2. Discriminação do objeto:

LOTE 1					
ITEM	**Código SIAD**	**DESCRIÇÃO/ESPECIFICAÇÃO**	**QUANTIDADE**	**VALOR UNITÁRIO (R$)**	**VALOR TOTAL (R$)**
1	107492	Solução de segurança com funcionalidades de *Firewall*, Sistema de Prevenção de Intrusão (IPS), Redes Virtuais Privadas (VPN), Controle de Aplicações e Ameaças, Filtro de URL e Protocolo de Qualidade de Serviço (*QoS*) Integrados	1		
2	107506	Serviços de atualização e suporte técnico (subscrição) para a solução de *Firewall*.	1		
3	107514	Serviços de instalação, configuração, testes em produção e ajustes dos equipamentos/produtos da solução *Firewall*	1		
4	107590	Serviços de treinamento da solução *Firewall*	1		

LOTE 2					
ITEM	**Código SIAD**	**DESCRIÇÃO/ESPECIFICAÇÃO**	**QUANTIDADE**	**VALOR UNITÁRIO (R$)**	**VALOR TOTAL (R$)**
Único	1816470	Servidor para Solução de Segurança	4		

2. **CLÁUSULA SEGUNDA – VIGÊNCIA**

2.1. Este contrato tem vigência por 12 (doze) meses, a partir da publicação de seu extrato no Diário Oficial do Estado de Minas Gerais.

2.2. Haverá possibilidade de prorrogação do item 2 do lote 1 que trata da prestação de serviços de suporte, garantia e atualização da solução *Firewall,* podendo ser prorrogado por idêntico período até o limite máximo de 48 (quarenta e oito) meses, mediante celebração de termos aditivos, conforme dispõe o art. 57, IV da lei n.º 8.666/93, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos: *(preencher de acordo com o lote a ser adjudicado)*

2.2.1. Os serviços tenham sido prestados regularmente;

2.2.2. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

2.2.3. Seja comprovado que o valor do contrato permanece economicamente vantajoso para a Administração;

2.2.4. Seja comprovado que o contratado mantém as condições iniciais de habilitação;

2.2.5. Haja manifestação expressa da CONTRATADA informando o interesse na prorrogação;

2.2.5.1. A CONTRATADA não tem direito subjetivo à prorrogação contratual.

2.2.6. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

3. **CLÁUSULA TERCEIRA – PREÇO**

3.1. O valor do presente Termo de Contrato é de R$ [inserir valor] ([inserir valor por extenso]) (preencher de acordo com o(S) Lote(S))

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4. **CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA**

4.1. A despesa decorrente desta contratação correrá por conta da (s) dotação(ões) orçamentária(s), e daquelas que vierem a substituí-las:

1191 04 126 115 2052 0001 4490 4006 e 1191 04 126 115 2052 0001 4490 5207, fontes 10.1 e/ou 48.1, 1191 04 126 115 2052 0001 3390 3921, 1191 04 126 115 2052 0001 3390 4002 e 1191 04 126 115 2052 0001 3390 3953 fonte 10.1.

4.2. No(s) exercício(s) seguinte(s), correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

5. **CLÁUSULA QUINTA – PAGAMENTO**

5.1. O prazo para pagamento e demais condições a ele referentes encontram-se no Edital e no Termo de Referência.

6. **CLÁUSULA SEXTA – REAJUSTE**

6.1. Durante o prazo de vigência, os preços contratos no Lote 1, itens 1, 3, e 4, e para o item único do Lote 2 não poderão ser reajustados monetariamente. *(preencher de acordo com o lote a ser adjudicado).*

6.2. Durante o prazo de vigência do Lote 1, o preços contratado no item 2 do Lote 1 poderá ser reajustado monetariamente com base no IPCA, observado o interregno mínimo de 12 meses, contados da apresentação da proposta, conforme disposto na Resolução Conjunta SEPLAG/SEF nº 8.898/2013 e nos arts. 40, XI, e 55, III, da Lei nº 8.666/93, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

6.2.1. O direito a que se refere o item 7.2 deverá ser efetivamente exercido mediante pedido formal da CONTRATADA até 180 dias após o atingimento do lapso de 12 meses a que se refere o caput desta cláusula sob pena de preclusão do direito ao seu exercício.

6.2.2. Nos reajustes subsequentes ao primeiro, manter-se-á o marco inicial descrito no item 6.1.

6.2.3. Desde que devidamente justificado e expressamente previsto no termo aditivo, o direito ao reajuste poderá ser exercido em momento posterior, até o encerramento do vínculo contratual.

6.3. Os efeitos financeiros retroagem à data do pedido apresentado pela CONTRATADA, observando-se o prazo prescricional de 5 anos.

7. CLÁUSULA SÉTIMA - ENTREGA E RECEBIMENTO DO OBJETO

7.1. As condições de entrega e recebimento do objeto são aquelas previstas no Termo de Referência.

8. CLÁUSULA OITAVA - FISCALIZAÇÃO

8.1. A fiscalização da execução do objeto será efetuada por Comissão/Representante especialmente designado pela CONTRATANTE no Termo de Designação de Gestor e Fiscal, na forma estabelecida pelo Termo de Referência.

9. CLÁUSULA NONA - DO MODO DE FORNECIMENTO

9.1. O modo de fornecimento dos bens a serem entregues pela CONTRATADA é aquele previsto no Termo de Referência e no Edital.

10. CLÁUSULA DÉCIMA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

10.1. As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas no Termo de Referência e no Edital.

11. CLÁUSULA DÉCIMA PRIMEIRA - DA FRAUDE E CORRUPÇÃO

11.1. Nos procedimentos licitatórios realizados pelo Estado de Minas Gerais serão observadas as determinações que se seguem.

11.2. O Estado de Minas Gerais exige que os licitantes/contratados observem o mais alto padrão de ética durante a licitação e execução dos contratos. Em consequência desta política, define, com os propósitos dessa disposição, os seguintes termos:

11.2.1. “prática corrupta” significa a oferta, a doação, o recebimento ou a solicitação de qualquer coisa de valor para influenciar a ação de um agente público no processo de licitação ou execução do contrato;

11.2.2. “prática fraudulenta” significa a deturpação dos fatos a fim de influenciar um processo de licitação ou a execução de um contrato em detrimento do CONTRATANTE;

11.2.3. “prática conspiratória” significa um esquema ou arranjo entre os concorrentes (antes ou após a apresentação da proposta) com ou sem conhecimento do CONTRATANTE, destinado a estabelecer os preços das propostas a níveis artificiais não competitivos e privar o CONTRATANTE dos benefícios da competição livre e aberta;

11.2.4. “prática coercitiva” significa prejudicar ou ameaçar prejudicar, diretamente ou indiretamente, pessoas ou suas propriedades a fim de influenciar a participação delas no processo de licitação ou afetar a execução de um contrato;

11.2.5. “prática obstrutiva” significa:

11.2.5.1. destruir, falsificar, alterar ou esconder intencionalmente provas materiais para investigação ou oferecer informações falsas aos investigadores com o objetivo de impedir uma investigação do CONTRATANTE ou outro órgão de Controle sobre alegações de corrupção, fraude, coerção ou conspiração; significa ainda ameaçar, assediar ou intimidar qualquer parte envolvida com vistas a impedir a liberação de informações ou conhecimentos que sejam relevantes para a investigação; ou

11.2.5.2. agir intencionalmente com o objetivo de impedir o exercício do direito do CONTRATANTE ou outro órgão de Controle de investigar e auditar.

11.3. O Estado de Minas Gerais rejeitará uma proposta e aplicará as sanções previstas na legislação vigente se julgar que o licitante, diretamente ou por um agente, envolveu-se em práticas corruptas, fraudulentas, conspiratórias ou coercitivas durante o procedimento licitatório.

11.4. A ocorrência de qualquer das hipóteses acima elencadas, assim como as previstas no Anexo I da Portaria SDE nº 51 de 03 de julho de 2009, deve ser encaminhada à Controladoria Geral do Estado - CGE para denúncia à Secretaria de Desenvolvimento Econômico do Ministério da Justiça, para adoção das medidas cabíveis.

12. CLÁUSULA DÉCIMA SEGUNDA – SANÇÕES ADMINISTRATIVAS

12.1. As sanções referentes à execução do contrato são aquelas previstas no Edital e no Termo de Referência.

13. CLÁUSULA DÉCIMA TERCEIRA – RESCISÃO

13.1. O presente Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666/93, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo das sanções aplicáveis.

13.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

13.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

13.4. O termo de rescisão será precedido de relatório indicativo dos seguintes aspectos, conforme o caso:

13.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente

cumpridos;

13.4.2. Relação dos pagamentos já efetuados e ainda devidos;

13.4.3. Indenizações e multas.

13.5. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na contratação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

13.6. As partes entregarão, no momento da rescisão, a documentação e o material de propriedade da outra parte, acaso em seu poder.

13.7. No procedimento que visar à rescisão do vínculo contratual, precedida de autorização escrita e fundamentada da autoridade competente, será assegurado o devido processo legal, o contraditório e a ampla defesa, sem prejuízo da possibilidade de a CONTRATANTE adotar, motivadamente, providências acauteladoras, inclusive a suspensão da execução do objeto.

14. CLÁUSULA DÉCIMA QUARTA - ALTERAÇÕES

14.1. O presente contrato poderá ser alterado nos casos previstos pelo art. 65 de Lei n.º 8.666/93, desde que devidamente motivado e autorizado pela autoridade competente.

14.1.1. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.1.2. As supressões resultantes de acordo celebrado entre as partes CONTRATANTES poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS.

15.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais de licitações e contratos administrativos e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor - e normas e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

16.1. A publicação do extrato do presente instrumento, no Diário Oficial Eletrônico de Minas Gerais, correrá a expensas da CONTRATANTE, nos termos da Lei Federal nº 8.666 de 21/06/1993.

17. CLÁUSULA DÉCIMA SÉTIMA – FORO

17.1. As partes elegem o foro da Comarca de Belo Horizonte, Minas Gerais, para dirimir quaisquer dúvidas ou litígios decorrentes deste Contrato, conforme art. 55, § 2º da Lei nº 8.666/93.

E por estarem ajustadas, firmam as partes este instrumento assinado eletronicamente.

CONTRATANTE:

CONTRATADA:

TESTEMUNHA 01:

TESTEMUNHA 02:

Documento assinado eletronicamente por **Arilson Leandro Fernandes Correa Lopes**, **Diretor**, em 23/09/2021, às 10:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **34218044** e o código CRC **B218EE4F**.

GOVERNO DO ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
Diretoria de Aquisições e Contratos/Divisão de Aquisições

Termo de Confidencialidade SEF/SPGF-DAC-AQUISIÇÕES nº. 34/2021

Belo Horizonte, 24 de agosto de 2021.

ANEXO VI

TERMO DE CONFIDENCIALIDADE

PREGÃO ELETRÔNICO Nº 1191001 - 48/2021

CELEBRANTE:

NOME: ESTADO DE MINAS GERAIS/SECRETARIA DE ESTADO DE FAZENDA
SEDE: Cidade Administrativa Tancredo Neves – Órgão: Secretaria de Estado de Fazenda – Prédio Gerais – 6º andar – Lado Ímpar - Rodovia Papa João Paulo II, nº 4.001, Bairro Serra Verde, no Município de Belo Horizonte/MG – CEP 31630-901.
CNPJ: 16.907.746/0001-13
REPRESENTANTE LEGAL: Lindenberg Naffah Ferreira, Superintendente de Tecnologia da Informação, credenciado na forma da Resolução nº. 3.597, de 03/12/2004.

CELEBRADA:

NOME EMPRESARIAL:
ENDEREÇO:
CNPJ:
INSCRIÇÃO ESTADUAL:
REPRESENTANTE(s) LEGAL(is):
NOME:
CPF:
NOME:
CPF:

CONSIDERANDO que a CELEBRADA contratou com o CELEBRANTE a aquisição de solução de segurança com funcionalidades de *Firewall*, Sistema de Prevenção de Intrusão (IPS), Redes Virtuais Privadas (VPN), Controle de Aplicações e Ameaças, Filtro de URL e Protocolo de Qualidade de Serviço (QoS) Integrados e servidores para substituição dos equipamentos ora em uso na SEF-MG, assim como serviços de atualização, garantia, instalação, suporte, e treinamento para o ambiente de Data Center, (***preencher de acordo com o lote adjudicado***), para uso da Secretaria de Estado de Fazenda de Minas Gerais, originário do Pregão Eletrônico nº 1191001 -

48/2021;

CONSIDERANDO que para tanto a CELEBRADA receberá informações a respeito do negócio, sistemas e/ou equipamentos, sendo de natureza peculiar as atividades do CELEBRANTE,

RESOLVEM as partes firmar o presente Termo de Confidencialidade, que se regerá pelas cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA - DAS DEFINIÇÕES

I - Para os fins deste instrumento, entende-se por informação: os dados, os documentos e os materiais que lhe sejam pertinentes. A "informação" poderá se revestir da forma oral, escrita, ou qualquer outra, corpórea ou não, a exemplo de: fórmulas, algoritmos, processos, projetos, croquis, fotografias, plantas, desenhos, conceitos de produto, especificações, amostras de ideia, nomes de fornecedores, preços e custos, definições e informações de negócios.

II - É considerada informação sigilosa toda e qualquer informação ou dado fornecido, comunicado ou revelado à CELEBRADA, seja know-how e dados, seja de caráter técnico ou não, que esteja em poder da CELEBRANTE e que seja revelado à CELEBRADA por necessidade de execução do trabalho contratado.

III - Toda a informação que a CELEBRADA tenha acesso ou que lhe seja fornecida pelo CELEBRANTE, será considerada sigilosa, salvo se estiver expressamente estipulado em contrário.

IV - Não será considerada sigilosa a:

a) informação identificada como de domínio público;
b) informação que se encontrava na posse legítima da CELEBRADA, livre de qualquer obrigação de sigilo, antes de sua revelação pelo CELEBRANTE;
c) informação expressamente identificada pelo CELEBRANTE como “não sigilosa”.

CLÁUSULA SEGUNDA – DAS OBRIGAÇÕES

As partes acordam:

a) não comercializar, divulgar, ceder, emprestar, revelar ou distribuir informação referente ao trabalho realizado, desde que autorizado pelo CELEBRANTE.

b) manter salvaguardas adequadas e seguras contra destruição, perda ou alteração dos arquivos de dados que o CELEBRANTE possa entregar à CELEBRADA, os quais ficarão sujeitos aos mesmos cuidados, proteção e segurança, dispensados àqueles da própria CELEBRADA, ficando esta livre e isenta de quaisquer responsabilidades em casos fortuitos ou de força maior;

c) respeitar e cumprir todas as estipulações referentes ao sigilo das informações;

d) devolver, independentemente de solicitação da outra parte, toda informação, sob qualquer forma que ela se encontre, bem como quaisquer cópias que eventualmente tenha em seu poder, após o término dos trabalhos sob contrato;

e) manter em absoluta segurança e devidamente protegidos todo e qualquer programa de computador, documentação correlata, material e/ou informação com dados sigilosos, ou que venham a ter conhecimento, obrigando-se, ainda, por si,

seus funcionários ou agentes e usuários, a não divulgar e nem revelar a terceiros quaisquer informações, sem prévia autorização escrita.

CLÁUSULA TERCEIRA - DA IMPOSSIBILIDADE DE DIVULGAÇÃO DAS INFORMAÇÕES

Pelo presente Termo, a CELEBRADA reconhece a natureza sigilosa da informação que lhe será transmitida, sob forma escrita, oral, em meio magnético ou qualquer outra forma de acesso, pelo CELEBRANTE e compromete-se a:

a) manter sob absoluto sigilo todas as informações que lhe forem transmitidas, visando à execução dos trabalhos contratados;

b) responsabilizar-se integralmente pelos atos de seus empregados, praticados nas dependências do CELEBRANTE, ou mesmo fora delas, que venham a causar danos a esta ou a seus funcionários, com a substituição imediata daqueles que não corresponderem ao padrão de comportamento exigido;

c) permitir o acesso à informação apenas aos seus funcionários ou prepostos, que necessitem absolutamente de conhecê-la para os fins referidos, comunicando-lhes antecipadamente as obrigações assumidas em matéria de sigilo e impondo-lhes o seu cumprimento;

d) não utilizar informações do CELEBRANTE em benefício próprio ou de terceiros;

e) proteger as informações de divulgação a terceiros com o mesmo grau de cautela com que protege suas próprias informações de importância similar, tendo em vista a natureza dos negócios do CELEBRANTE;

f) assegurar que, durante a execução dos serviços, seus empregados façam uso de crachás contendo o nome, a função e a denominação;

g) credenciar junto ao CELEBRANTE todo o seu pessoal designado para a execução dos serviços, objeto deste Termo, sob pena de não lhe ser permitido o acesso às instalações;

h) comunicar ao CELEBRANTE qualquer alteração relativa à titularidade ou gestão;

i) instruir os encarregados, responsáveis pelo tratamento das informações confidenciais, a proteger e manter o sigilo das mesmas.

Parágrafo Primeiro

A CELEBRADA, para fins de sigilo, obriga-se por seus administradores, empregados e contratados.

Parágrafo Segundo

A obrigação de sigilo mantém-se, mesmo após o termo da vigência do contrato, só cessando após autorização escrita do CELEBRANTE.

CLÁUSULA QUARTA – DO DESCUMPRIMENTO

I - O não cumprimento do compromisso de sigilo, estabelecido neste instrumento, sujeitará a CELEBRADA ao pagamento das perdas e danos sofridos pelo CELEBRANTE, sem prejuízo das demais sanções legais cabíveis, decorrentes da violação deste Termo.

II - O não exercício pelas partes de qualquer direito a ela assegurado neste Termo, ou a não aplicação de qualquer medida, penalidade ou sanção possível, não importará em renúncia ou novação, não devendo, portanto, ser interpretada como desistência de sua aplicação em caso de reincidência.

CLÁUSULA QUINTA - DO DESEMPENHO DAS FUNÇÕES

I - O presente Termo obriga as partes e seus sucessores.

II - A Superintendência de Tecnologia da Informação/ Diretoria de Infraestrutura e Soluções Tecnológicas - STI/DIST, acompanhará e fiscalizará o cumprimento deste Termo.

III - Este Termo não poderá ser modificado, alterado ou rescindido, no todo ou em parte, exceto por documento escrito assinado entre as Partes.

CLÁUSULA SEXTA - DO FORO

As partes elegem o foro da Comarca de Belo Horizonte - MG para dirimir quaisquer dúvidas ou litígios eventualmente surgidos em decorrência deste instrumento.

E, para firmeza e prova de assim haverem, entre si, ajustado e acordado, após ter sido lido juntamente com o Contrato, o presente instrumento é assinado eletronicamente pelas partes.

CELEBRANTE: ESTADO DE MINAS GERAIS/SECRETARIA DE ESTADO DE FAZENDA

CELEBRADA:

Testemunha 1:

Testemunha 2:

Documento assinado eletronicamente por **Arilson Leandro Fernandes Correa Lopes**, **Diretor**, em 23/09/2021, às 10:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

SECRETARIA DE ESTADO DE FAZENDA

Diretoria de Aquisições e Contratos/Divisão de Aquisições

Versão v.20.09.2020.

ANEXOS

ANEXO VII

AVALIAÇÃO DE FORNECEDORES

1. DA AVALIAÇÃO DE DESEMPENHO DO FORNECEDOR

A CONTRATADA estará sujeita à avaliação de seu desempenho na execução do objeto quanto aos critérios de prazo, quantidade, qualidade e documentação, nos termos da Resolução SEPLAG nº 13/2014.

1.1. Critério Prazo

O critério Prazo avalia o cumprimento das datas previamente definidas na autorização de fornecimento e respectivos agendamentos para a entrega do(s) objeto(s) e possui a pontuação assim distribuída, de acordo com o desempenho da CONTRATADA:

a) 30 (trinta) pontos, se a entrega for realizada na data agendada e conforme prazo previsto na autorização de fornecimento;

b) 28 (vinte e oito) pontos, se a entrega for realizada em desacordo com a data agendada, mas ainda conforme prazo previsto na autorização de fornecimento;

c) 22 (vinte e dois) pontos, se a entrega for realizada com atraso de até 15 (quinze) dias, contados a partir do término do prazo previsto na autorização de fornecimento;

d) 10 (dez) pontos, se a entrega for realizada com atraso de 16 (dezesseis) a 30 (trinta) dias, contados a partir do término do prazo previsto na autorização de fornecimento; ou

e) 0 (zero) ponto, se a entrega for realizada com atraso superior a 30 (trinta) dias, contados a partir do término do prazo previsto na autorização de fornecimento.

I- Na hipótese de reagendamento da data da entrega por solicitação da CONTRATADA, esta será pontuada com a totalidade dos pontos, caso o reagendamento ocorra antes da data anteriormente agendada e a entrega seja realizada:

a) conforme nova data agendada; e

b) dentro do prazo limite previsto na autorização de fornecimento.

II - Na hipótese do não cumprimento da data agendada e/ou o prazo limite previsto

na autorização de fornecimento, por caso fortuito ou força maior, a CONTRATADA poderá apresentar justificativa para o atraso na entrega, que será analisada pelo responsável pelo recebimento, podendo ser aceita ou não.

III - Na hipótese de a justificativa mencionada no inciso anterior ser aceita pelo responsável pelo recebimento, a CONTRATADA será pontuada com a totalidade dos pontos.

IV – O reagendamento da entrega após o prazo máximo de entrega definido na autorização de fornecimento não afasta a sujeição da CONTRATADA à aplicação de multa sobre o valor considerado em atraso e, conforme o caso, a outras sanções estabelecidas na Lei e neste instrumento.

V – Em caso de irregularidade não sanada pela CONTRATADA, a CONTRATANTE reduzirá a termo os fatos ocorridos para aplicação de sanções.

1.2. Critério Quantidade

O critério Quantidade avalia o cumprimento da entrega do(s) objeto(s) relativamente à quantidade definida na autorização de fornecimento e possui a pontuação assim distribuída de acordo com o desempenho da CONTRATADA:

a) 30 (trinta) pontos, se a quantidade recebida for igual à quantidade solicitada;

b) 28 (vinte e oito) pontos, se a quantidade recebida for maior que a quantidade solicitada;

c) 22 (vinte e dois) pontos, se a quantidade recebida for maior ou igual a 75% (setenta e cinco por cento) e menor que 100% (cem por cento) da quantidade solicitada;

d) 10 (dez) pontos, se a quantidade recebida for maior ou igual a 50% (cinquenta por cento) e menor que 75% (setenta e cinco por cento) da quantidade solicitada; ou

e) 0 (zero) ponto, se a quantidade recebida for inferior a 50% (cinquenta por cento) da quantidade solicitada.

I – A CONTRATADA é obrigada a entregar o quantitativo total solicitado, devendo ser aceito quantitativo menor apenas em hipóteses excepcionais, devidamente justificadas e em função do atendimento ao interesse público.

II – A aceitação de quantitativo menor que o estabelecido em autorização de fornecimento não afasta a sujeição da CONTRATADA à aplicação de sanções estabelecidas na Lei e neste instrumento.

III – Se houver recusa do recebimento em virtude de desconformidade entre o quantitativo de materiais entregues e a quantidade estabelecida na Autorização de Fornecimento (AF), essa será registrada em eventual entrega posterior, referente à mesma autorização de fornecimento, na qual o fornecedor terá prejuízo em sua nota.

IV - Na hipótese do não cumprimento do quantitativo previsto na autorização de fornecimento, por caso fortuito ou força maior, a CONTRATADA poderá apresentar justificativa para o atraso na entrega, que será analisada pelo responsável pelo recebimento, podendo ser aceita ou não.

V - Na hipótese de a justificativa mencionada no inciso anterior ser aceita pelo responsável pelo recebimento, a CONTRATADA será pontuada com a totalidade dos pontos.

1.3. Critério Qualidade

O critério Qualidade avalia o cumprimento da entrega do(s) objeto(s) relativamente às

exigências de especificação técnica, e possui a pontuação assim distribuída de acordo com o desempenho da CONTRATADA:

a) 30 (trinta) pontos, se a qualidade for aprovada;

b) 22,5 (vinte e dois vírgula cinco) pontos, se a qualidade for aprovada com ressalva de baixa criticidade; ou

c) 10 (dez) pontos, se a qualidade for aprovada com ressalva de alta criticidade.

d) 0 (zero) pontos, se houver desconformidade total entre os materiais recebidos e a especificação técnica exigida.

I - As ressalvas referidas nas alíneas “b” e “c” deste subitem 1.3 não deverão comprometer a qualidade exigida nem a utilidade do material.

II – Se houver recusa do recebimento em virtude de desconformidade entre os materiais recebidos e a especificação técnica exigida, esta será registrada em eventual entrega posterior, referente à mesma autorização de fornecimento.

III – Na hipótese do inciso anterior, a CONTRATADA receberá a pontuação 0 (zero) nesse critério.

O critério Qualidade avalia o cumprimento da entrega do(s) objeto(s) relativamente às exigências de especificação técnica e embalagem de material, aos quais serão atribuídas pontos de acordo com o desempenho da CONTRATADA.

I – O subcritério “Embalagem” avalia as condições da embalagem do material e possui a pontuação assim distribuída de acordo com o desempenho da CONTRATADA:

a) 10 (dez) pontos, se a embalagem for aprovada; ou

b) 5 (cinco) pontos, se a embalagem for aprovada com ressalva.

II – Se houver recusa do recebimento em virtude de embalagem inadequada do material, esta será registrada em eventual entrega posterior, referente à mesma autorização de fornecimento.

III – Na hipótese do inciso anterior, a CONTRATADA receberá a pontuação 0 (zero) no subcritério “Embalagem”.

IV - O subcritério “Especificação técnica” avalia a conformidade entre os materiais recebidos e a especificação técnica exigida, possui a pontuação assim distribuída de acordo com o desempenho da CONTRATADA:

a) 20 (vinte) pontos, se a qualidade for aprovada;

b) 15 (quinze) pontos, se a qualidade for aprovada com ressalva de baixa criticidade; ou

c) 6,6 (seis vírgula seis) pontos, se a qualidade for aprovada com ressalva de alta criticidade.

V – Se houver recusa do recebimento em virtude de desconformidade entre os materiais recebidos e a especificação técnica exigida, esta será registrada em eventual entrega posterior, referente à mesma autorização de fornecimento.

VI – Na hipótese do inciso anterior, a CONTRATADA receberá a pontuação 0 (zero) no subcritério “Especificação técnica”.

VII – A ressalva referida na alínea “b” do inciso I e nas alíneas “b” e “c” do inciso IV deste subitem 1.3 não deverão comprometer a qualidade exigida nem a utilidade do material.

1.4. Critério Documentação

O critério Documentação avalia o cumprimento da entrega do(s) objeto(s) relativamente à regularidade da Nota Fiscal, e possui a pontuação assim distribuída de acordo com o desempenho da CONTRATADA:

a) 10 (dez) pontos, se a Nota Fiscal tiver a sua validade atestada;

b) 0 (zero) ponto, se a Nota Fiscal apresentar irregularidade(s) que impeçam o ateste de sua validade.

I - Para atestar a validade da Nota Fiscal, deverá ser verificada a conformidade dos seguintes itens:

a) Dados do órgão/entidade que realizou a compra;

b) Valores unitários e totais;

c) Descrição do produto em conformidade com o item de material solicitado e com o material entregue;

d) Quantidade constante na nota em conformidade com a quantidade solicitada;

e) Inexistência de rasuras; e

f) Outros elementos solicitados pelo órgão ou entidade no instrumento convocatório.

O critério Documentação avalia o cumprimento da entrega do(s) objeto(s) relativamente à regularidade da Nota Fiscal e dos documentos adicionais apresentados, aos quais serão atribuídas pontos de acordo com o desempenho da CONTRATADA.

I - O subcritério “Nota Fiscal” avalia a regularidade da Nota Fiscal e possui a pontuação assim distribuída de acordo com o desempenho da CONTRATADA:

a) 5 (cinco) pontos, se a Nota Fiscal tiver a sua validade atestada;

b) 0 (zero) ponto, se a Nota Fiscal apresentar irregularidade(s) que impeça(m) o ateste de sua validade.

II - Para atestar a validade da Nota Fiscal, deverá ser verificada a conformidade dos seguintes itens:

a) Dados do órgão/entidade que realizou a compra;

b) Valores unitários e totais;

c) Descrição do produto em conformidade com o item de material solicitado e com o material entregue;

d) Quantidade constante na nota em conformidade com a quantidade solicitada;

e) Inexistência de rasuras; e

f) Outros elementos solicitados pelo órgão ou entidade no instrumento convocatório.

III - O subcritério “Documentos Adicionais” avalia a regularidade e conformidade dos documentos específicos relativos ao material(is) entregue(s) com a legislação aplicável e possui a pontuação assim distribuída de acordo com o desempenho da CONTRATADA:

a) 5 (cinco) pontos, se a documentação adicional estiver em conformidade com a legislação aplicável ao objeto; ou

b) 0 (zero) ponto, se a documentação adicional apresentar inconformidades.

2. DO INDICADOR DE DESEMPENHO DO FORNECEDOR

Os registros de desempenho da CONTRATADA conforme os critérios do item 1 deste Anexo, serão a base para o cálculo do seu respectivo indicador de desempenho.

I - O indicador de desempenho da CONTRATADA poderá ser apresentado nas seguintes formas:

a) Indicador de Desempenho do Fornecedor por Entrega (IDF-E): será calculado para um determinado item da autorização de fornecimento, a partir da soma das pontuações atribuídas em cada critério de avaliação;

b) Indicador de Desempenho do Fornecedor por Autorização de Fornecimento (IDF-AF): será calculado a partir da média aritmética simples dos IDF-E, no âmbito de uma mesma autorização de fornecimento;

c) Indicador de Desempenho do Fornecedor por Contratação (IDF-C): será calculado a partir da média aritmética simples dos IDF-AF, no âmbito desta contratação.

3. DAS AÇÕES QUE PODERÃO SER TOMADAS EM RELAÇÃO AO DESEMPENHO DA CONTRATADA

I - Conforme resultado obtido no Indicador de Desempenho do Fornecedor por Contratação (IDF-C), a CONTRATADA obterá os seguintes conceitos:

a) “A”, se o seu aproveitamento for maior que 90% (noventa por cento);

b) “B”, se o seu aproveitamento for maior que 70% (setenta por cento) e menor ou igual a 90% (noventa por cento); ou

c) “C”, se o seu aproveitamento for menor ou igual a 70% (setenta por cento).

II - A CONTRATANTE poderá adotar as seguintes ações, conforme o conceito obtido pela CONTRATADA no Indicador de Desempenho do Fornecedor por Contratação (IDF-C), nos termos do inciso anterior:

a) Conceito “A”: avaliar a possibilidade de gerar atestado de capacidade técnica;

b) Conceito “B”: notificar a CONTRATADA para correção da(s) falta(s) e/ou realizar reuniões com a CONTRATADA para analisar as causas do baixo desempenho, bem como solicitar que a CONTRATADA elabore proposta de plano de ação corretivo para validação da CONTRATANTE; e

c) Conceito “C”: além das medidas previstas no conceito “B”, avaliar a possibilidade de abertura de processo administrativo punitivo para aplicação das sanções dispostas nos anexos do Edital.

III - A CONTRATANTE poderá adotar as ações previstas na alínea “b” do inciso anterior caso a CONTRATADA obtenha pontuação igual ou abaixo de 90% (noventa por cento) em 1 (uma) avaliação referente ao índice de desempenho do fornecedor por entrega (IDF-E).

IV - A CONTRATANTE poderá adotar as ações previstas na alínea “c” do inciso II deste item 3 caso a CONTRATADA obtenha pontuação igual ou abaixo de 90% (noventa por cento) em 2 (duas) avaliações, consecutivas ou não, referentes ao índice de desempenho do fornecedor por entrega (IDF-E).

V - O disposto neste Anexo não exclui a notificação ou a aplicação de sanções administrativas à CONTRATADA nas hipóteses previstas na Lei Federal nº 8.666/1993, Lei Federal nº 10.520/2002, Lei Estadual nº 13.994/2001, Lei Estadual n° 14.167/2002 e Decreto Estadual nº 45.902/2012, bem como as dispostas nos anexos do Edital.

Documento assinado eletronicamente por **Arilson Leandro Fernandes Correa Lopes**, **Diretor**, em 23/09/2021, às 10:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **34218198** e o código CRC **74E22BF4**.

Referência: Processo nº 1190.01.0010082/2021-93 SEI nº 34218198

Rodovia Papa João Paulo II, 4001 - Edifício Gerais - Bairro Serra Verde - Belo Horizonte - CEP 31630-901