



GOVERNO DO DISTRITO FEDERAL
INSTITUTO DE GESTÃO ESTRATÉGICA DE SAÚDE DO DISTRITO FEDERAL
Núcleo de Compras Diversas e Serviços

EDITAL DO CHAMAMENTO Nº 034/2024

O Instituto de Gestão Estratégica de Saúde do Distrito Federal – IGESDF, pessoa jurídica de direito privado, constituída sob a forma de Serviço Social Autônomo (SSA), regulamentado por meio do Decreto nº 39.674, de 20 de fevereiro de 2019, sediado no TR SIA TRECHO 17 RUA 06 LOTE 115, ZONA INDUSTRIAL (GUARÁ), BRASÍLIA-DF, CEP: 71.200-216, por meio da Gerência de Compras, torna público para o conhecimento dos interessados que realizará processo de contratação, na forma eletrônica, do tipo **MENOR PREÇO GLOBAL**, visando a **Contratação de empresa especializada na prestação de serviços de conectividade em SD-WAN para interligação das Unidades da CONTRATANTE por meio de uma rede de dados, incluindo o gerenciamento e a segurança da rede (todos por demanda)**, de acordo com as especificações, quantidades e demais condições constantes neste Edital e seus anexos para atender às necessidades do Instituto de Gestão Estratégica de Saúde do Distrito Federal - IGESDF, nos termos do Regulamento Próprio de Compras e Contratações do IGESDF, aprovado pela Portaria Nº 611 do Conselho de Administração, publicado na Pag. 25 do DODF Nº 181, conforme Resolução CA/IGESDF nº 04/2022.

1. DO OBJETO

1.1. O presente processo de contratação tem por objeto a contratação de empresa especializada na prestação de serviços de conectividade em SD-WAN para interligação das Unidades da CONTRATANTE por meio de uma rede de dados, incluindo o gerenciamento e a segurança da rede. (todos por demanda), para atendimento às demandas do IGESDF, **conforme descrição detalhada indicada no subitem 20 do Elemento Técnico - ANEXO I deste Edital**, para atender às necessidades das unidades de saúde administradas pelo Instituto de Gestão Estratégica de Saúde do Distrito Federal – IGESDF, conforme condições estabelecidas neste Edital e seus anexos.

2. DO PRAZO PARA ACOLHIMENTO DE PROPOSTAS

2.1. O período de acolhimento das propostas será de 05 (cinco) dias úteis, contados da publicação do Edital no site oficial do IGESDF (www.igesdf.org.br).

3. DO REGRAMENTO

3.1. Este processo de compras e contratação respeitará o disposto no Regulamento Próprio de Compras e Contratações do IGESDF, disponível no endereço eletrônico [Regulamento de Compras 2022 - IGESDF](#).

4. DAS CONDIÇÕES PARA PARTICIPAÇÃO

4.1. Poderão participar dos processos de compras e contratações do IGESDF, as pessoas naturais e jurídicas brasileiras ou estrangeiras legalmente autorizadas a funcionar no Brasil, as quais possuam regularidade jurídica, fiscal e trabalhista em plena vigência.

4.2. As compras ou contratações de âmbito internacional ajustar-se-ão às diretrizes estabelecidas pelos órgãos federais responsáveis pela política monetária e pela política de comércio exterior.

4.3. Todos os documentos emitidos em língua estrangeira deverão ser acompanhados de tradução juramentada e estar dentro do prazo de validade.

4.4. Fica vedada a participação nos processos de compras e contratações, conforme vedações previstas nos incisos I a V do artigo 5º da Resolução SEI-GDF nº 04/2022:

4.4.1. Dirigente ou empregado do IGESDF, incluindo os membros da Diretoria Executiva e dos Conselhos de Administração, Fiscal;

4.4.2. Servidor público ou detentor de cargo em comissão ou função comissionada ou gratificada, no âmbito da Secretaria de Estado de Saúde do Distrito Federal - SES/DF, que possa ter conflito de interesse com o IGESDF, na execução do

contrato de gestão firmado com o Poder Executivo, por intermédio da SES/DF;

4.4.3. Parentes consanguíneos ou afins até o terceiro grau de pessoas elencadas nos Subitens 4.4.1 e 4.4.2;

4.4.4. Empresas apenas com suspensão pelo IGESDF;

4.4.5. Pessoas jurídicas nas quais as pessoas elencadas nos subitens 4.4.1 e 4.4.2 tenham participação.

4.4.5.1. Entende-se como participação societária a titularidade individual direta, como acionista, detentor de mais de 0,3% (três décimos por cento) no capital social de sociedade por ações e como sócio detentor de cota superior a 2% (dois por cento) no capital social das demais modalidades empresariais.

4.4.5.2. O participante deverá apresentar declaração expressa, conforme modelo apresentado no ANEXO III deste edital ou similar, atestando que não se enquadra nos casos dos subitens 4.4.1 a 4.4.5.

5. DAS DISPOSIÇÕES PRELIMINARES

5.1. Este Edital e seus anexos serão publicados no site oficial do IGESDF (www.igesdf.org.br), bem como na plataforma de compras **APOIO COTAÇÕES** (<https://www.apoiocotacoes.com.br>), podendo ocorrer ainda, a publicação do Extrato do Edital em outras formas de divulgação, a exemplo de:

5.1.1. Diário Oficial do Distrito Federal;

5.1.2. Redes sociais;

5.1.3. Jornais de grande circulação;

5.1.4. Mensagem Eletrônica a potenciais fornecedores.

6. DO PEDIDO DE ESCLARECIMENTO

6.1. A partir da publicação do Edital no site do IGESDF e na plataforma de compras, os interessados terão até o terceiro dia útil que antecede ao término do período de acolhimento das propostas, para enviar pedidos de esclarecimentos ou questionamentos técnicos sobre a aquisição/contratação.

6.2. Os pedidos deverão ser enviados ao Núcleo de Compras, por meio do endereço eletrônico: compras.servicos@igesdf.org.br, informando no campo assunto o número do ID da cotação.

7. DA APRESENTAÇÃO DAS PROPOSTAS DE PREÇOS

7.1. O participante deverá **cadastrar o preço da cotação** e anexar a documentação de habilitação na plataforma de compras, por meio do sistema eletrônico no site da plataforma de cotação, até a data e horário definidos.

7.2. A informação dos dados para acesso deve ser feita na página inicial do site de cotação nos campos específicos para login e senha.

7.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais na plataforma 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.

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

7.5. Não será aceita, no mesmo item ou lote, a participação de duas ou mais empresas com os mesmos sócios e/ou representantes legais.

7.6. O participante será responsável por todas as transações efetuadas em seu nome, assumindo como firme e verdadeira sua proposta de preços.

7.7. Os valores deverão ser apresentados em moeda corrente nacional e deverão estar inclusos todos os custos operacionais, frete, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que indicam direta ou indiretamente no fornecimento do produto.

7.8. Serão consideradas **02 (duas) casas decimais após a vírgula** para os preços unitários e totais;

7.9. A proposta apresentada terá validade de 90 (noventa) dias, contados da data de encerramento da cotação;

7.10. Deverá ser ofertada uma única cotação, com uma única apresentação, com preços unitários e totais por item.

7.11. O item ofertado deve estar em conformidade com as especificações solicitadas na plataforma de compras, no ID da cotação vinculado à este Edital, devendo ser informado uma única marca e/ou fabricante e quando couber, informar

modelo e/ou referência.

- 7.12. Não haverá sessão pública para abertura das propostas recebidas.
- 7.13. Prevalecerão no caso de divergências, as informações do preço unitário sobre o total, os valores por extenso sobre os numéricos e o **preço cadastrado na plataforma de compras sobre a proposta escrita**.
- 7.14. Serão desclassificadas as propostas de preços que não atenderem às exigências do presente Edital e seus anexos, forem omissas ou apresentarem irregularidade insanáveis, tais como: valores manifestamente inexequíveis, exorbitantes, iguais a zero ou acima dos preços praticados no mercado.
- 7.15. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências para que a empresa comprove a exequibilidade da proposta. Entende-se por preços inexequíveis os que forem inferiores ao custo de produção, acrescidos dos encargos legais, hipótese em que o proponente será convocado para demonstrar a exequibilidade do preço ofertado. Caso não seja demonstrada a viabilidade ou o proponente for omissos, a proposta será desclassificada em decisão fundamentada.
- 7.16. Encerrado o prazo de cotação na plataforma, proceder-se-á com a publicação, no sítio institucional do IGESDF, da relação nominal dos concorrentes.
- 7.17. O participante não relacionado que comprovar ter cadastrado tempestivamente a cotação na plataforma de compras, terá o prazo de 01 (um) dia útil para solicitar sua inclusão na relação nominal dos concorrentes.
- 7.18. No mesmo prazo do subitem anterior, contado da publicação da relação nominal dos concorrentes, os participantes do Chamamento que cadastraram a cotação na plataforma poderão atualizar ou complementar os documentos de habilitação exigidos neste Edital.
- 7.19. A apresentação da proposta implicará a tácita admissão de que a documentação técnica e os esclarecimentos prestados foram suficientes para que os serviços sejam executados nas condições estipuladas pelo contrato e seus anexos.

8. DA DOCUMENTAÇÃO DE HABILITAÇÃO

- 8.1. Para habilitação dos proponentes e seguimento da classificação das propostas, será exigida a seguinte documentação:
- 8.2. **Declaração expressa, conforme modelo apresentado no ANEXO I deste Edital, atestando que não se enquadra nas vedações previstas nos incisos I a V do artigo 5º da Resolução SEI-GDF nº 04/2022.**
- 8.3. **Habilitação Jurídica:**
- 8.4. Cópia da Cédula de identidade, quando se tratar de Pessoa Física;
- 8.5. CNPJ – Comprovante de inscrição e de situação cadastral no Cadastro Nacional de Pessoa Jurídica;
- 8.6. Registro comercial ou Contrato Social em vigor, devidamente registrado e/ou alteração, em se tratando de Sociedades Comerciais, e no caso de Sociedades por Ações, acompanhado de documentos de eleição de seus administradores;
- 8.7. Licença de Funcionamento ou Alvará de Localização;
- 8.8. **Referentes à Habilitação Técnica:**
- 8.9. Apresentar os documentos exigidos no **subitem 25 do Elemento Técnico** - Anexo I deste Edital.

9. DO CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

- 9.1. Será adotado o critério de **MENOR PREÇO GLOBAL**, no julgamento das propostas que atendam adequadamente a descrição do objeto e as condições de participação do Chamamento.

10. PRAZO PARA ENTREGA

- 10.1. Conforme subitem 22 do Elemento Técnico - Anexo I deste Edital.

11. UNIDADE NA QUAL O PRODUTO DEVERÁ SER ENTREGUE

- 11.1. Conforme subitem 23 do Elemento Técnico - Anexo I deste Edital.

12. DA NEGOCIAÇÃO

- 12.1. O Núcleo de Compras efetivará a publicação, no sítio institucional do IGESDF, do resultado preliminar do certame, contendo o valor da menor proposta.
- 12.2. Após a publicação do resultado preliminar, será aberto prazo de 01 (um) dia útil para negociação, no qual todas as concorrentes poderão manifestar interesse em reduzir o valor ofertado para patamar inferior ao vencedor provisório, devendo apresentar, no mesmo prazo, a proposta negociada.
- 12.2.1. Não será admitida proposta apresentada intempestivamente.
- 12.3. Na fase de negociação, poderá ser solicitada a prorrogação do prazo de validade da proposta apresentada.
- 12.4. Na análise de aceitabilidade do preço ofertado, poderão ser solicitadas à empresa participante cópias de notas fiscais emitidas a, no máximo, 90 (noventa) dias ou contratos vigentes com outras empresas.
- 12.5. Na impossibilidade de apresentação de notas fiscais emitidas a, no máximo, 90 (noventa) dias ou contratos vigentes, a empresa deverá apresentar declaração, conforme modelo apresentado no ANEXO IV deste Edital, informando os motivos e atestando que os preços praticados são compatíveis com os preços de mercado, sob pena de incorrer na prática do crime previsto no art. 299 do Código Penal.
- 12.6. Após a fase de negociação será declarada vencedora a empresa que apresentar a melhor proposta negociada, obedecendo aos critérios definidos.
- 12.7. Quando houver empate entre duas ou mais empresas qualificadas, será solicitada a renegociação, com prazo de 04 (quatro) horas para retorno da proposta renegociada.
- 12.8. Permanecendo a situação de empate, serão utilizados ordenadamente os seguintes critérios:
- 12.8.1. Primeiro: Maior quantidade de itens com menor preço aprovados no processo;
- 12.8.2. Segundo: Empresa nacional;
- 12.8.3. Terceiro: Empresa com maior tempo de atividade no mercado;
- 12.8.4. Quarto: Sorteio.
- 12.9. Em caso de utilização do quarto critério, o sorteio será realizado por comissão constituída de no mínimo 03 (três) membros funcionários do IGESDF, que registrará o fato em Ata e esta por sua vez passará a ser parte integrante do processo.
- 12.10. Nos casos em que a empresa participante com a proposta mais vantajosa não atender às exigências e condições deste Edital e seus anexos, o Núcleo de Compras examinará a proposta subsequente na ordem de classificação, sucessivamente, até a apuração de uma proposta que atenda completamente a todos os requisitos exigidos.

13. **DOS RECURSOS**

- 13.1. Será publicada no sítio institucional do IGESDF a Ata Final de Resumo de Compras/Contratações, na qual constará o histórico do processo.
- 13.2. Do resultado final caberá recurso administrativo, a ser interposto no prazo de 02 (dois) dias corridos, contados da publicação da Ata Final de Resumo de Compras. O prazo que, porventura, se encerrar em dia em que não haja expediente na área administrativa do IGESDF será prorrogado para o primeiro dia útil subsequente.
- 13.3. Os recursos deverão ser enviados ao Núcleo de Compras, por meio do endereço eletrônico: compras.servicos@igesdf.org.br, informando no campo assunto o número da cotação.
- 13.4. A falta de manifestação do fornecedor de interpor recurso importará na decadência do direito de sua apelação.
- 13.5. Não havendo recurso quanto à declaração de vencedor, o objeto será adjudicado ao concorrente melhor classificado, encaminhando o processo para homologação da autoridade superior.

14. **DA HOMOLOGAÇÃO**

- 14.1. Concluída a etapa de seleção de fornecedores com o fornecedor adjudicado, a autoridade competente procederá a homologação do processo.
- 14.2. Todos os avisos pertinentes a esse processo de aquisição/contratação serão publicados no site oficial do IGESDF (www.igesdf.org.br), não podendo os interessados alegar desconhecimento da informação.

15. **DO INSTRUMENTO CONTRATUAL**

- 15.1. Homologado o resultado do processo de compras, será realizada a análise da seguinte documentação:
- 15.2. Cópia do Documento de Identidade e CPF do Representante Legal da empresa.
- 15.3. Se a empresa se fizer representar por procurador, faz-se necessário o encaminhamento do instrumento público ou particular, neste último caso, com firma reconhecida em cartório.
- 15.4. União – Certidão Negativa de regularidade com a Fazenda Federal, mediante certidão conjunta negativa de débitos, ou positiva com efeitos de negativa, relativos aos tributos federais e à Dívida Ativa da União;
- 15.5. CNDT – Certidão Negativa de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante Certidão Negativa de Débitos Trabalhistas, ou certidão positiva com efeitos de negativa;
- 15.6. FGTS – Certidão Negativa de regularidade relativa ao Fundo de Garantia do Tempo de Serviço, mediante Certificado de Regularidade;
- 15.7. Certidão Negativa de regularidade perante as Fazendas Municipal, Estadual ou Distrital da sede do CONTRATADA;
- 15.8. CEIS – Cadastro Nacional de Empresas Inidôneas e Suspensas, mantido pela Controladoria Geral da União;
- 15.9. CNJ – Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça;
- 15.10. TCU – Lista de Inidôneos, mantida pelo Tribunal de Contas da União; e
- 15.11. Certidão Negativa de Falência ou Concordata (art.192, Lei nº11.101/2005), Recuperação Judicial ou Extrajudicial e Execução patrimonial, expedidas pelo setor de distribuição da Justiça Comum, Justiça Federal e Justiça do Trabalho do domicílio ou domicílios da pessoa física ou jurídica. Caso a participante esteja em processo de recuperação judicial, impossibilitada de atender a presente solicitação, deverá a mesma comprovar que efetivamente encontra-se em tal situação, devendo para tanto, apresentar certidão positiva ou documento capaz de demonstrar tal circunstância. Restando demonstrado que a participante encontra-se em recuperação judicial, tal situação não será motivo ensejador de inabilitação e consequente desclassificação, permitindo a sua participação no Chamamento Público, desde que atendidas as demais exigências e demonstrada a sua capacidade econômica para a execução do contrato.
- 15.12. A empresa cadastrada no Sistema de Cadastro Unificado de Fornecedores do Ministério do Planejamento poderá encaminhar declaração do SICAF/SIASG em substituição às certidões elencadas nos subitens 15.4 a 15.7.
- 15.13. A empresa poderá enviar o extrato da Consulta de Situação de Pessoa Jurídica presente no portal do TCU em substituição aos subitens 15.8 a 15.10.
- 15.14. A Gerência de Contratos poderá manter banco de fornecedores com a documentação descrita no item anterior atualizada ou solicitar o envio ao fornecedor vencedor do Chamamento.
- 15.15. O vencedor deverá providenciar seu cadastro de usuário externo na plataforma SEI – conforme instruções apresentadas no Anexo III deste edital, tendo o prazo de até 05 (cinco) dias corridos, contados a partir da data de sua convocação, para assinar o instrumento contratual ou aceitar os termos equivalentes - Anexo IV, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas no Regulamento de Compras e Contratações do IGESDF.
- 15.16. Na hipótese de o vencedor não possuir a documentação prevista no item 15.1 ou não assinar o instrumento contratual no prazo estabelecido, o IGESDF poderá convocar a próxima empresa classificada de acordo com a Ata Final Resumo de Compras, respeitando a ordem de classificação, para firmar o instrumento contratual.
- 15.17. A vigência do Instrumento Contratual será de 30 meses, a contar de sua assinatura, podendo ser prorrogado, por igual período, mediante a Termo Aditivo até o limite máximo de 60 (sessenta) meses, conforme preconiza o Regulamento Próprio de Compras e Contratações do IGESDF.
- 15.18. A partir da assinatura do instrumento contratual ou aceite dos termos, a contratada deverá iniciar o fornecimento do objeto de acordo com o informado no chamamento e subitem 10.1 deste Edital, conforme quantidades solicitadas.
- 15.19. A contratada se obriga a manter o fornecimento de bens e serviços, caso exista risco a vida dos pacientes, por no mínimo 90 (noventa) dias ou até a celebração de contrato com outro fornecedor.
- 15.20. A referida vigência não exonera o fornecedor do cumprimento da garantia mínima do(s) produto(s), contados a partir da data do termo de recebimento definitivo do objeto.

16. DO PAGAMENTO

- 16.1. Os pagamentos à empresa que vier a ser contratada neste processo, serão feitos nos termos previstos no Instrumento Contratual, consoante os preços estabelecidos na proposta de preço, e observadas as disposições deste Edital e seus Anexos, **em até 30 (trinta) dias corridos** após o recebimento do produto a contento e emissão do documento fiscal válido em nome do IGESDF, com todos os campos preenchidos discriminando valor unitário e total do item, sem rasuras,

devidamente atestados pelo funcionário responsável pelo recebimento do produto, constando, ainda, o número do banco, da agência e da conta corrente onde deseja receber seu crédito.

17. DAS DISPOSIÇÕES GERAIS

- 17.1. O acompanhamento dos atos processuais deverá ser feito por meio do site <https://www.igesdf.org.br/>.
- 17.2. Não serão considerados os documentos que não estiverem de acordo com as condições deste Edital e seus anexos, quer por omissão, quer por discordância.
- 17.3. Poderá o IGESDF revogar ou anular qualquer ato constitutivo ou derivado neste processo de aquisição/contratação, no todo ou em parte, por conveniência administrativa e interesse público devidamente justificado, sem que caiba ao fornecedor direito à indenização, salvo em caso de dano efetivo disso resultante e na forma da lei.
- 17.4. O IGESDF poderá valer-se de pareceres técnicos e/ou jurídicos exarados por empregado/comissão devidamente constituídos, para embasar sua decisão quando do julgamento das fases de habilitação e proposta.
- 17.5. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação da empresa que o tiver apresentado, ou, caso tenha sido vencedora, poderá implicar na rescisão do contrato, sem prejuízo das demais sanções cabíveis.
- 17.6. É facultado ao IGESDF, em qualquer fase do processo de aquisição/contratação, promover diligências com vistas a esclarecer ou a complementar a instrução do mesmo, vedada a inclusão posterior de documento ou informação que deveria constar originalmente na proposta.
- 17.7. O fornecedor convocado para prestar qualquer esclarecimento adicional deverá fazê-lo no prazo determinado, sob pena de desclassificação/inabilitação.
- 17.8. Na contagem dos prazos, excluir-se-á o dia do início e incluir-se-á o do vencimento, e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário.
- 17.9. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça o recebimento das documentações na data marcada, o prazo será automaticamente transferido para o primeiro dia útil subsequente, no mesmo horário e local, anteriormente estabelecidos, desde que não haja comunicação em contrário.
- 17.10. Os casos não previstos neste Edital serão decididos pela Autoridade Competente do IGESDF.
- 17.11. A empresa participante/contratada deverá manter seus dados sempre atualizados em todos os canais disponíveis de comunicação.
- 17.12. O descumprimento total ou parcial das obrigações assumidas caracterizará a inadimplência do fornecedor e/ou do detentor, sujeitando-o às penalidades previstas no Regulamento Próprio de Compras e Contratações do IGESDF e no instrumento contratual.
- 17.13. O foro designado para julgamento de quaisquer questões judiciais resultante deste Edital de Chamamento será o da circunscrição judiciária de Brasília-DF.

18. ANEXOS

- 18.1. Fazem parte integrante do presente Edital os anexos a seguir listados:

Anexo I	Elemento Técnico
Anexo II	Modelo de Declaração de não vínculo
Anexo III	Modelo de Declaração de preços
Anexo IV	Instrução de acesso Externo ao SEI -
Anexo V	Minuta de Contrato -

ANEXO I AO EDITAL 034/2024 - ELEMENTO TÉCNICO

INFORMAÇÕES EXTRAÍDAS DO ELEMENTO TÉCNICO Nº 5/2024 - IGESDF/DALOG/SUTCS/GEINF/NUTEL - Doc SEI
([140823598](#))

ELEMENTO TÉCNICO

Nº 5/2024 - IGESDF/DALOG/SUTCS/GEINF/NUTEL

19. DO OBJETO

19.1. O presente Elemento Técnico tem por objeto a contratação de empresa especializada na prestação de **serviços de conectividade em SD-WAN para interligação das Unidades da CONTRATANTE por meio de uma rede de dados, incluindo o gerenciamento e a segurança da rede. (todos por demanda)**, para atendimento às demandas do IGESDF, constantes neste Elemento Técnico, para atender às necessidades do Hospital de Base do Distrito Federal - IGESDF.

19.2. A solução será composta por 1 ITEM dispostos da seguinte forma:

Unidade do IGESDF	Velocidade mínima do Link de Internet	QNTD.de NFGW do TIPO 1	QNTD.de NFGW do TIPO 2	LICENÇA
Hospital de Base – HB	1Gbps	2		PREMIUM
Hospital Regional de Santa Maria – HRSM	1Gbps	2		PREMIUM
Hospital Cidade do Sol - HSOL	300 Mbps		1	PREMIUM
PO700	300 Mbps		1	PREMIUM
SIA	300 Mbps		1	PREMIUM
UPA – Ceilândia	100 Mbps		1	PREMIUM
UPA - Núcleo Bandeirante	100 Mbps		1	PREMIUM
UPA - Recanto das Emas	100 Mbps		1	PREMIUM
UPA - São Sebastião	100 Mbps		1	PREMIUM
UPA – Samambaia	100 Mbps		1	PREMIUM
UPA – Sobradinho	100 Mbps		1	PREMIUM
UPA – Brazlândia	100 Mbps		1	PREMIUM
UPA – Ceilândia (Setor O)	100 Mbps		1	PREMIUM
UPA – Gama	100 Mbps		1	PREMIUM
UPA – Paranoá	100 Mbps		1	PREMIUM

UPA – Planaltina	100 Mbps		1	PREMIUM
UPA – Riacho Fundo II	100 Mbps		1	PREMIUM
UPA – Vicente Pires	100 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 1 (sob demanda)	2Gbps	1		PREMIUM
Unidade do IGESDF Tipo 2 (sob demanda)	1Gbps	1		PREMIUM
Unidade do IGESDF Tipo 3 (sob demanda)	600 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 4 (sob demanda)	300 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 5(sob demanda)	100 Mbps		1	PREMIUM

20. ESPECIFICAÇÃO DETALHADA DO OBJETO A SER CONTRATADO

- 20.1. Especificação detalhada e quantidades, conforme:
- 20.2. Anexo I: Solução de SD-WAN;
- 20.3. Anexo II: Proposta;
- 20.4. Anexo III: Ordem de Fornecimento;
- 20.5. Anexo IV: Fiscal do Contrato e seu respectivo Substituto;
- 20.6. Anexo V: Endereço IGESDF;

21. JUSTIFICATIVA PARA A AQUISIÇÃO E/OU CONTRATAÇÃO DO SERVIÇO

21.1. O Serviço Social Autônomo, Instituto Hospital de Base do Distrito Federal – IHB, instituído por determinação do Decreto nº 38.332, de 13 de julho de 2017, conforme autorização da Lei Distrital nº 5.899, de 3 de julho de 2017, celebrou o Contrato de Gestão Nº 001/2018, com a Secretaria de Estado de Saúde do Distrito Federal, com isso o IHB reveste-se da atribuição de administrar a unidade de saúde Hospital de Base do Distrito Federal, sendo responsável por garantir o pleno funcionamento de suas atividades funcionais e operacionais.

21.2. Considerando a Lei 6.270, de 31 de janeiro de 2019, que alterou a Lei 5.899, de 13 de julho de 2017 para modificar o nome do Instituto Hospital de Base do Distrito Federal – IHBDF para Instituto de Gestão Estratégica do Distrito Federal – IGESDF,

21.3. Considerando que o IGESDF foi regulamentado pelo Decreto 39.674, de 20 de fevereiro de 2019, que ampliou a sua atuação assistencial para incluir sob sua gestão, além do Hospital de Base, o Hospital Regional de Santa Maria (HRSA) e as Unidades de Pronto Atendimento (UPAS).

21.4. Com o aumento das aplicações que necessitam de conectividade de rede de dados no IGESDF, faz-se necessária a contratação de links que permitam interligar as unidades de interesse do IGESDF para efetuar tráfego de voz, dados e imagem, com garantia de qualidade de serviço e segurança da informação, além de proporcionar uma melhor gestão contratual, mantendo a padronização da solução adotada.

21.5. O alinhamento entre a solução apresentada e o PDTI 2024-2026 encontra-se registrado na necessidade NT08 - Plano de Reestruturação da infraestrutura de TI e tendo como meta: Criar uma infraestrutura sólida, que consiga manter o ambiente em funcionamento e propicie seu crescimento de acordo com as necessidades atuais e futuras, através da manutenção do parque instalado e uma política de crescimento e inovação das tecnologias utilizadas.

21.6. O sistema de telecomunicações do IGESDF, referente a links de comunicação, atualmente contratados estão operando sem redundância, o que gera degradação nos serviços acesso ao sistema web de gestão hospitalar MV Soul, no acesso à internet, na comunicação entre as unidades do IGESDF e instabilidade no serviço de telefonia VoIP. Vários destes, além de críticos, necessitam de conexões que garantam alta disponibilidade, pois devem estar em funcionamento permanentemente, durante as 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, durante os 365 (trezentos e sessenta e cinco) dias do ano, uma vez que falhas ou instabilidades no sistema de telecomunicação, por se tratar de Hospitais e UPAs, impactam diretamente nas áreas assistenciais e administrativas, dificultando o cumprimento da missão institucional do IGESDF.

21.7. Para atender às necessidades de Negócio nos padrões de atendimento atualmente contratados, deve-se considerar os seguintes níveis mínimos de serviço e características de contratação:

- a) Razão Social da Contratada;
- b) Número e vigência do contrato se for o caso;
- c) Objeto do contrato;
- d) Declaração de que foram atendidas as expectativas quanto ao cumprimento de cronogramas pactuados;
- e) Local e Data de Emissão;
- f) Identificação do responsável pela emissão do atestado;
- g) Cargo, Contato (telefone e correio eletrônico);
- h) Assinatura do responsável pela emissão do atestado;
- i) Devem ser originais ou autenticados, se cópias, e legíveis;

21.8. Contratação de prestação de serviços de conectividade de longa distância para interligação das Unidades do IGESDF, por intermédio de uma rede de dados programável e automatizada que controla o tráfego de forma dinâmica e segura, com base em políticas de aplicativos, condições de rede ou prioridade do circuito de comunicação, utilizando Solução SD-WAN (Software-Defined Wide Area Network), incluindo o Gerenciamento da Solução SD-WAN, a Gerência de Nível de Serviço (GNS) e a cooperação técnica.

21.9. Mediante ao exposto, o objeto desta contratação visa a melhoria no sistema de telecomunicação do IGESDF, com a contratação do serviço de SD-WAN, que ira interligar as unidades IGESDF, com solução de segurança de dados e monitoramento para detecção e antecipação de possíveis falhas ou instabilidades na rede, e investigar se há algum imprevisto de segurança no intuito de evitar ameaças digitais que possam comprometer toda a infraestrutura do IGESDF.

22. **PRAZO DESEJADO PARA ENTREGA DO BEM E A PREVISÃO DE VIGÊNCIA CONTRATUAL**

22.1. A primeira reunião de alinhamento, será realizada após 5 dias após assinatura do contrato.

22.2. Os equipamentos e acessórios devem ser entregues no prazo de até 60 (sessenta) dias corridos, a contar da assinatura do contrato.

22.3. O contrato terá sua vigência pelo prazo de 30 (trinta) meses, a contar de sua assinatura, podendo ser prorrogado, por igual período, mediante a Termo Aditivo até o limite máximo de 60 (sessenta) meses, conforme preconiza o Regulamento Próprio de Compras e Contratações do IGESDF.

23. **UNIDADE NA QUAL O BEM DEVERÁ SER ENTREGUE E/OU O SERVIÇO DEVERÁ SER PRESTADO**

23.1. O endereço das unidades do IGESDF, está disponível no ANEXO V.

24. **INDICAÇÃO DO FISCAL DO CONTRATO, E SEU RESPECTIVO SUBSTITUTO**

24.1. A informação referente ao Fiscal do contrato e seu respectivo substituto está disponível no ANEXO IV.

25. **DOCUMENTOS DE QUALIFICAÇÃO TÉCNICA :**

25.1. **COMPROVAÇÃO DA QUALIFICAÇÃO TÉCNICA:**

25.2. Atestado (s) de capacidade técnica, fornecido (s) por pessoa (s) jurídica (s) de direito público ou privado, para as quais o CONTRATADO tenha executado o fornecimento da solução com a complexidade operacional equivalente aos especificados neste Elemento Técnico.

25.3. Serão aceitos somente atestados expedidos após a conclusão do contrato ou decorrido no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior.

25.4. A empresa participante deve disponibilizar, quando demandada, todas as informações necessárias à comprovação da legitimidade do atestado, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços

25.5. Os atestados deverão ser emitidos em papel timbrado e conter:

25.6. Razão Social, CNPJ e Endereço Completo da Empresa Emitente;

- a) Razão Social da Contratada;
- b) Número e vigência do contrato se for o caso;
- c) Objeto do contrato;
- d) Declaração de que foram atendidas as expectativas quanto ao cumprimento de cronogramas pactuados;
- e) Local e Data de Emissão;
- f) Identificação do responsável pela emissão do atestado;

- g) Cargo, Contato (telefone e correio eletrônico);
- h) Assinatura do responsável pela emissão do atestado;
- i) Devem ser originais ou autenticados, se cópias, e legíveis;

25.7. No caso de apresentação de atestado de empresas privadas, não serão considerados aqueles apresentados por empresas participantes do mesmo grupo empresarial da contratada. Serão consideradas como de mesmo grupo, empresas controladas pela contratada, ou que tenham pelo menos uma pessoa física ou jurídica que seja sócia da empresa emitente e da contratada.

25.8. Será aceito o somatório de atestados para comprovar a capacidade técnica e operacional, desde que reste demonstrada a execução concomitante dos contratos

26. **DO CRITÉRIO DE JURALMENTO DAS PROPOSTAS:**

26.1. Atendidos todos os requisitos estabelecidos neste Elemento Técnico, será contratada a empresa que apresentar o MENOR PREÇO GLOBAL, e atenda as qualificações deste instrumento, nos termos do Regulamento de Compras e Contratações do IGESDF.

27. **ANEXO I DO ELEMENTO TÉCNICO – SOLUÇÃO SD-WAN**

27.1. **INFORMAÇÕES GERAIS:**

27.2. A prestação dos serviços de conectividade abrange circuitos de comunicação, hardwares e softwares, com as respectivas licenças de uso, assim como instalações, desinstalações, dimensionamentos, configurações, testes, operação, monitoração, gerenciamento, suporte técnico e manutenção.

27.3. O gerenciamento pretendido abrange as funcionalidades do Gerenciamento da Solução SD-WAN e da GNS.

27.4. A rede interligará as Unidades da CONTRATANTE, distribuídas conforme relação indicada em anexo V, a qual contempla nome da Unidade, endereço completo, CEP, banda em Mbps e Gbps, bem como novas unidades que vierem a ser requisitadas pela CONTRATANTE, dada a possibilidade de expansão da sua estrutura, mediante prévia análise de custos a ser efetuada pela CONTRATADA, tendo como base os valores vigentes à época da assinatura do Contrato.

27.5. A prestação dos serviços de conectividade deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, por 365 (trezentos e sessenta e cinco) dias do ano, durante toda a vigência do contrato.

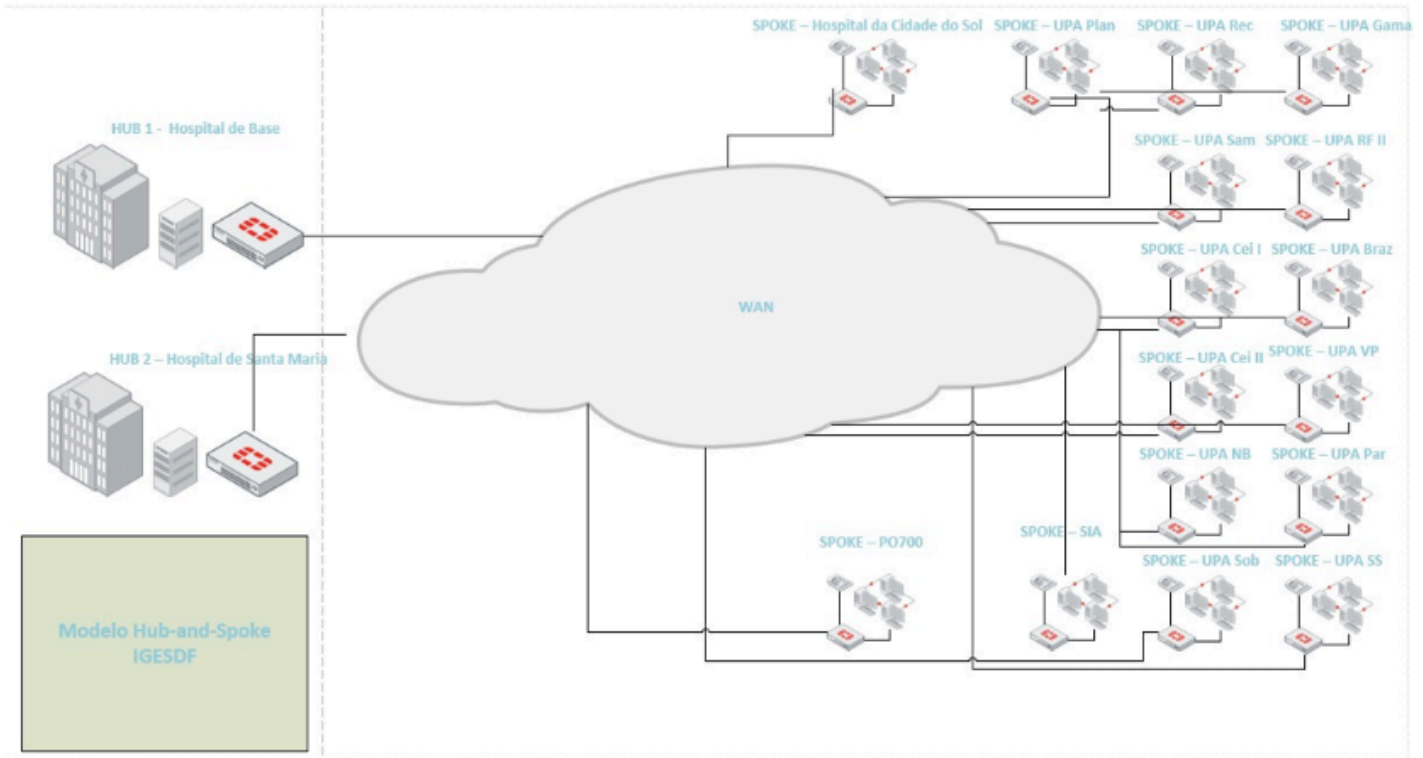
27.6. A Solução de SD-WAN contempla a disponibilização de link de internet e equipamento de Next Generation Firewall (NGFW), de forma que as especificações técnicas, suporte técnico, Service Level Agreement (SLA) e referencial de Glosa, estão disponíveis no ANEXO II

27.7. **TOPOLOGIA FÍSICA:**

27.8. A rede deverá prover a interligação entre as Unidades da CONTRATANTE, utilizando Solução SD-WAN via Internet Pública, de acordo com a arquitetura que atende às necessidades da Administração Pública contratante.

27.9. **TOPOLOGIA LÓGICA:**

27.10. A rede deverá prover a interligação entre as Unidades da CONTRATANTE, utilizando Solução SD-WAN via Internet Pública, de modo a permitir a conectividade dessas unidades, conforme exemplificado na Figura abaixo:



27.11. A rede de dados deverá suportar topologia par full-mesh ou parcial mesh em todas as Unidades da CONTRATANTE deverão ter conectividade direta, via túnel VPN, com os N (19) Datacenters referentes a cada unidade do IGESDF.

27.12. As Unidades da CONTRATANTE deverão ter conectividade direta, via tunelamento, com a(s) sua(s) correspondente(s) unidade(s) hierárquica(s).

27.13. O limite de atuação da CONTRATADA, para cada Unidade da CONTRATANTE, é(são) a(s) porta(s) do switch(es) LAN da CONTRATANTE, na qual a CONTRATADA deverá conectar o(s) cabo(s) proveniente(s) de sua rede e, caso necessário, fornecer a(s) interface(s) e o(s) conversor(es) de mídia.

27.14. A CONTRATADA, disponibilizará informações referente ao SNMP configurado em todos os equipamentos que forem instalados no ambiente da CONTRATANTE para fins de monitoramento dos mesmos.

27.15. A CONTRATANTE será responsável pela configuração lógica do(s) seu(s) switch(es) e roteador(es) LAN.

27.16. A CONTRATADA efetuará a instalação no prazo de até 90 (noventa) dias, a partir da data da aprovação do Projeto Executivo pelo CONTRATANTE.

27.17. Em até 05 (cinco) dias corridos após a assinatura do contrato, a CONTRATANTE deverá realizar reunião inicial do contrato.

27.18. Em até 07 (sete) dias corridos após a realização da reunião inicial, a CONTRATADA deverá entregar um Projeto Executivo, contendo, no mínimo:

27.19. Definição de topologia física e lógica;

- a) Definição de topologia física e lógica;
- b) Plano de Implantação e Migração da Rede;
- c) Cronograma de Implantação da Rede;
- d) Plano de Endereçamento;
- e) Plano de balanceamento do tráfego;
- f) Dimensionamento de enlaces e interfaces de comunicação.

27.20. A elaboração do Projeto Executivo contará com a participação da CONTRATADA e CONTRATANTE.

27.21. **SD-WAN**

27.22. Todos os itens relacionados no anexo I, serão executados sob demanda da **CONTRATANTE**, podendo ser descontinuados a qualquer momento sem ônus ao IGESDF.

27.23. A Solução de SD-WAN contempla a disponibilização de link de internet e equipamento de Next Generation Firewall (NGFW), de forma que as especificações técnicas, suporte técnico, Service Level Agreement (SLA) e Obrigações da Contratada, estão disponíveis a seguir:

27.24. Tabela Solução SD-WAN:

Unidade do IGESDF	Velocidade mínima do Link de Internet	QNTD.de NFGW do TIPO 1	QNTD.de NFGW do TIPO 2	LICENÇA
Hospital de Base – HB	1Gbps	2		PREMIUM
Hospital Regional de Santa Maria – HRSM	1Gbps	2		PREMIUM
Hospital Cidade do Sol - HSOL	300 Mbps		1	PREMIUM
PO700	300 Mbps		1	PREMIUM
SIA	300 Mbps		1	PREMIUM
UPA – Ceilândia	100 Mbps		1	PREMIUM
UPA - Núcleo Bandeirante	100 Mbps		1	PREMIUM
UPA - Recanto das Emas	100 Mbps		1	PREMIUM
UPA - São Sebastião	100 Mbps		1	PREMIUM
UPA – Samambaia	100 Mbps		1	PREMIUM
UPA – Sobradinho	100 Mbps		1	PREMIUM
UPA – Brazlândia	100 Mbps		1	PREMIUM
UPA – Ceilândia (Setor O)	100 Mbps		1	PREMIUM
UPA – Gama	100 Mbps		1	PREMIUM
UPA – Paranoá	100 Mbps		1	PREMIUM
UPA – Planaltina	100 Mbps		1	PREMIUM
UPA – Riacho Fundo II	100 Mbps		1	PREMIUM
UPA – Vicente Pires	100 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 1 (sob demanda)	2 Gbps	1		PREMIUM
Unidade do IGESDF Tipo 2 (sob demanda)	1 Gbps	1		PREMIUM
Unidade do IGESDF Tipo 3 (sob demanda)	600 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 4 (sob demanda)	300 Mbps		1	PREMIUM
Unidade do IGESDF Tipo 5(sob demanda)	100 Mbps		1	PREMIUM

27.25. **ESPECIFICAÇÃO DO LINK DE INTERNET:**

27.26. A solução de Link de Internet, inicialmente deverá ser disponibilizado sobre demanda conforme Tabela abaixo:

Unidade do IGESDF	Velocidade mínima do Link de Internet
Hospital de Base – HB	1Gbps

Hospital Regional de Santa Maria – HRSM	1Gbps
Hospital Cidade do Sol - HSOL	300 Mbps
PO700	300 Mbps
SIA	300 Mbps
UPA – Ceilândia	100 Mbps
UPA - Núcleo Bandeirante	100 Mbps
UPA - Recanto das Emas	100 Mbps
UPA - São Sebastião	100 Mbps
UPA – Samambaia	100 Mbps
UPA – Sobradinho	100 Mbps
UPA – Brazlândia	100 Mbps
UPA – Ceilândia (Setor O)	100 Mbps
UPA – Gama	100 Mbps
UPA – Paranoá	100 Mbps
UPA – Planaltina	100 Mbps
UPA – Riacho Fundo II	100 Mbps
UPA – Vicente Pires	100 Mbps
Unidade do IGESDF Tipo 1 (sob demanda)	2 Gbps
Unidade do IGESDF Tipo 2 (sob demanda)	1 Gbps
Unidade do IGESDF Tipo 3 (sob demanda)	600 Mbps
Unidade do IGESDF Tipo 4 (sob demanda)	300 Mbps
Unidade do IGESDF Tipo 5(sob demanda)	100 Mbps

27.27. O serviço internet deverá ser disponibilizado pela CONTRATADA com a utilização de protocolo IP e concessão de 1 (um) bloco cidr/27 para cada hospital , 1 (um) bloco cidr/29 para cada unidade (UPAS, PO700 e SIA), link adicional TIPO 1 e TIPO2 1 (um) bloco cidr/27 para cada link solicitado e link adicional TIPO 3, TIPO 4 e TIPO 5 1 (um) bloco cidr/29 para cada link solicitado.

27.28. Os Links de Internet deverão ser redundantes e possuir rotas e caminhos distintos.

27.29. A CONTRATADA deverá fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os equipamentos e recursos que forem necessários para o provimento do serviço telecomunicação do IGESDF, especificado neste Elemento Técnico.

27.30. Os equipamentos serão de propriedade da CONTRATADA que deverá ser responsável pelo suporte técnico dos mesmos, cumprindo com os tempos de atendimento estabelecidos neste Elemento Técnico;

27.31. A CONTRATADA deverá fornecer o acesso através de meio físico (fibra ótica) instalado diretamente no local indicado pela CONTRATANTE.;

27.32. O serviço a ser fornecido pela empresa a ser contratada deverá, minimamente:

- 27.33. Possuir suporte a DNS (resolução direta e reversa), inclusive ao protocolo DNSSEC.
- 27.34. Utilizar exclusivamente fibra óptica desde as instalações da empresa a ser contratada até as instalações da Contratante.
- 27.35. Suportar QoS (Quality of Service – Qualidade de Serviço).
- 27.36. Suportar Tráfego de Videoconferência e Voz sobre IP (VoIP) em todos os componentes e enlaces da rede e em todos os componentes da Solução.
- 27.37. Permitir métodos de priorização de tráfego;
- 27.38. Utilizar protocolos e padrões internacionais da IEEE, IETF e ITU.
- 27.39. Suportar NAT.
- 27.40. Suportar LAN Switching: VLAN.
- 27.41. Possibilitar que o equipamento a ser disponibilizado para a perfeita execução dos serviços possa ser instalado em rack de 19" da CONTRATANTE.
- 27.42. Fornece todo o material e equipamentos necessários para a instalação e operação dos links, como cabos/fibras, tubulações, sistema de aterramento, sistema de proteção contra descarga elétrica e atmosférica, rádios, modems, roteadores, adaptadores etc.
- 27.43. **ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO (mínima):**
- 27.44. Será de responsabilidade da CONTRATADA fornecer todos os equipamentos e meios necessários à plena prestação dos serviços, excluindo-se o fornecimento de energia elétrica para alimentação dos equipamentos nas dependências das unidades, o aterramento da rede e a climatização das dependências.
- 27.45. CONTRATADA deverá garantir que a disponibilidade, a segurança, o desempenho e a qualidade do serviço prestado estejam dentro dos limites estabelecidos pela CONTRATANTE.
- 27.46. O serviço deve ter a disponibilidade de 99,5% (noventa e nove vírgula cinco por cento), a ser medido e entregue em relatórios mensalmente.
- 27.47. A CONTRATADA deverá fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os equipamentos/recursos que forem necessários para o provimento dos serviços, conforme solicitados nesta especificação. Os equipamentos serão de propriedade da CONTRATADA, que deverá ser responsável pelo suporte técnico dos mesmos.
- 27.48. Deverá ser feito balanceamento de carga dos links de internet de forma automática para garantir a alta disponibilidade dos links especificados neste Elemento Técnico.
- 27.49. A CONTRATADA deverá garantir que a disponibilidade, a segurança, o desempenho e a qualidade do serviço prestado estejam dentro dos limites estabelecidos pela CONTRATANTE.
- 27.50. Faz parte da prestação do serviço, além da porta de interconexão à Internet global de forma dedicada, o transporte do sinal da CONTRATADA até as instalações do CONTRATANTE.
- 27.51. A instalação do ponto de acesso físico no CONTRATANTE é de responsabilidade exclusiva da CONTRATADA e será cobrada apenas no momento da ativação do link.
- 27.52. A CONTRATADA deverá fornecer toda a infraestrutura de rede de telecomunicações necessária para disponibilizar os serviços IP para acesso à Internet global de forma dedicada e exclusiva (não compartilhada), com os circuitos de acesso com a mesma capacidade de tráfego nos dois sentidos.
- 27.53. A largura de banda deve sempre estar disponível na totalidade do fluxo contratado, respeitando-se o limiar desse Projeto Básico.
- 27.54. A CONTRATANTE, em acordo com a CONTRATADA, poderá solicitar adequações da capacidade dos enlaces com acréscimo/decrécimo sem ônus para o IGESDF.
- 27.55. Caso solicitado, a CONTRATADA deverá realizar alterações nas taxas de transmissão contratadas, com a adequação dos recursos necessários (roteadores, enlaces, backbone e outros) garantindo o alto desempenho do serviço sem ônus para o IGESDF.
- 27.56. O backbone da CONTRATADA deverá possuir interligação direta através de canais próprios e dedicados.
- 27.57. A CONTRATADA deverá fornecer um bloco de endereçamento Ipv4 ou IPv6 para a CONTRATANTE.
- 27.58. A CONTRATADA deverá obedecer às recomendações elaboradas pela ABNT para provimento de serviços de acesso à Internet (ISP).
- 27.59. Os circuitos empregados pela CONTRATADA deverão atender às Normas Técnicas Brasileiras e regulamentações da ANATEL, quando essas não entrarem em conflito com o especificado neste documento.

- 27.60. A CONTRATADA deverá manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados.
- 27.61. A CONTRATADA deverá aplicar e manter atualizados os patches de segurança nos seus roteadores ou em outros equipamentos de suas redes, exclusivos para a prestação de serviços à CONTRATANTE.
- 27.62. A CONTRATADA deverá realizar análises de vulnerabilidades periódicas nos seus segmentos da rede relacionados à prestação do serviço objeto desta especificação, visando detectar possíveis falhas de segurança da rede.
- 27.63. A CONTRATADA deverá auxiliar a equipe técnica do CONTRATANTE na identificação e mitigação de incidentes de segurança que comprometam a disponibilidade do serviço.
- 27.64. A CONTRATADA deverá fornecer roteador CPE com as seguintes características:
- a) O roteador CPE deverá ser dimensionado, fornecido, instalado, mantido, gerenciado e operado pela CONTRATADA e deverá ser garantido o desempenho e os níveis de serviços contratados;
 - b) O roteador CPE deverá ser dimensionado para atender o serviço na capacidade máxima de CPU especificada e de 70% de memória;
 - c) O roteador CPE deverá ser fornecido com todos os componentes, módulos e acessórios necessários ao seu perfeito funcionamento;
 - d) O roteador CPE deverá possuir, no mínimo, 04 (quatro) portas de LAN GigaBit ethernet com conector tipo RJ45 e SFP+ para cabos UTP e fibra ótica para conexão com a rede local da CONTRATANTE;
 - e) O roteador CPE deverá suportar classificação de tráfego de acordo com, pelo menos, os critérios de IP origem/destino e portas TCP/UDP. Também deverá suportar gerenciamento de filas com base em classes de tráfego.
 - f) A configuração lógica do roteador CPE será definida pela CONTRATADA com a aprovação da CONTRATANTE.
- 27.65. Em todas as unidades do IGESDF a CONTRATADA fornecerá e instalará os roteadores CPEs, equipados com no-break do tipo senoidal on-line com autonomia mínima de 30 (trinta) minutos e quaisquer equipamentos que se façam necessários, os quais ficarão fisicamente instalados nas mesmas dependências das redes locais.
- 27.66. Os roteadores CPE deverão ser fornecidos, instalados, mantidos, gerenciados e operados pela CONTRATADA e deverá ser garantido o desempenho e os níveis de serviços contratados.
- 27.67. Cada roteador CPE será fornecido com todos os acessórios e programas necessários à sua instalação, operação e monitoração (cabo de console, cabo de alimentação, cabo V35 e outros cabos e acessórios se fizerem necessários).
- 27.68. Todos os roteadores suportarão, além dos protocolos básicos para operação em uma rede IP, Frame Relay e PPP, com compressão de dados e o protocolo de roteamento OSPF. Com opção de security telnet e IP security (IPSec).
- 27.69. Os roteadores terão facilidades de configuração através de porta serial e da console de monitoramento.
- 27.70. O roteador de acesso à Internet deverá ter a seguinte configuração mínima:
- a) Possuir, no mínimo, 04 (quatro) portas de LAN GigaBit ethernet sendo 02 (duas) portas com conector tipo RJ45 para cabos UTP e 02 (duas) portas com conector tipo SFP+ para fibra ótica que seja compatível com o padrão IEEE 802.3;
 - b) Possuir opção de boot local e permitir armazenamento de firmware e configuração em memória compact flash que deverá ser fornecida caso seja necessário;
 - c) Possuir no mínimo 256 MB de memória flash ou similar e 2048 MB de memória DRAM, permitindo que o equipamento atenda a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do fabricante;
 - d) Possuir seu firmware e sistema operacional em versão que atenda a todos os requisitos mínimos necessários (memória, flash, dentre outros) para suportá-lo;
 - e) Suportar o protocolo de rede IP sobre ATM, compatível com a RFC 2684;
 - f) Suportar portas seriais Síncronas, Assíncronas, ATM OC3 e Gigabit;
 - g) Implementar os protocolos de roteamento OSPF (Open Shortest Path First) e BGP 4;
 - h) Implementar o protocolo de distribuição de endereços IP - DHCP Relay, Server, Client;
 - i) O protocolo IGMPv1, v2 e v3 (Internet Grouping Message Protocol), PIM-SM e PIM-DM;
 - j) Implementar, no mínimo, 32 VLAN (Virtual Local Area Network), com base em portas, endereços MAC e Padrão IEEE 802.1q;
 - k) Implementar NAT (Network Address Translation) e PAT (Port Address Translation);
 - l) Deverá suportar os padrões QoS (Quality-of-Service), 802.1p e 802.1q;
 - m) Disponibilizar, no mínimo, dois níveis de senha de acesso;
 - n) Deve possuir arquitetura modular, permitindo a substituição de interfaces e do módulo de processamento central;
 - o) Capacidade de comutação mínima de 1.400 (mil e quatrocentos) kbps disponível no equipamento;
 - p) Permitir a criação de funções de filtragem baseada em listas de controle de acesso com capacidade de filtrar através de endereços de origem e destino e porta UDP e TCP de origem e destino (ACL Básicas e Estendidas - Lista de controle de acesso) 3 mil linhas;
 - q) Deverá ser do mesmo fabricante e compartilhar a mesma sintaxe de comandos dos demais roteadores fornecidos;

- r) Deve possuir interfaces com velocidades iguais ou superiores às especificadas para os links fornecidos;
- s) Permitir a configuração remota através de TELNET, SSH e por porta console RJ-45. O equipamento deverá possuir, além da porta console, porta auxiliar que permita a ligação de modem externo;
- t) Deverá ser compatível com, pelo menos, um dos protocolos a seguir: NetFlow, NetStream ou IPFIX, de forma a permitir estatísticas mais apuradas do tráfego;
- u) Implementar IPSEC com criptografia em hardware. Devem ser suportados 1500 túneis externos IPSEC simultâneos, com capacidade mínima de 8 Mbps de tráfego criptografado em 3DES/MD5, considerando-se pacotes de 1400 bytes;
- v) Deve implementar a criação de túneis VPN dinamicamente, de forma a garantir que escritórios remotos criem túneis entre si sob demanda, mesmo quando associados a endereços IP dinâmicos.

27.71. **Anti-DDOS:**

27.72. A CONTRATADA deverá disponibilizar em seu backbone proteção contra-ataques de negação de serviços, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS e DDoS de acordo considerando os requisitos mínimos a seguir:

- a) Serviços deverão ter proatividade para solução e prevenção de incidentes e ataques;
- b) Monitorar disponibilidade e desempenho de todos os links de dados existentes nesse elemento técnico em regime de 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, durante os 365 (trezentos e sessenta e cinco) dias do ano utilizando profissionais de forma dedicada;
- c) Tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo pela contratada.
- d) A solução deve possuir a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.
- e) A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes malformados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras.

27.73. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo aos seguintes:

- a) Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;
- b) Ataques à pilha TCP, incluindo mal-uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;
- c) Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;
- d) Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);
- e) Ataques à camada de aplicação, incluindo protocolos HTTP e DNS.
- f) A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um determinado período considerado seguro pela CONTRATADA.
- g) A contratada deve mitigar ataques por 3 horas, caso o ataque ultrapasse o SLA de mitigação contratado.
- h) Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole,
- i) As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques.
- j) A CONTRATADA deve disponibilizar um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, durante os 365 (trezentos e sessenta e cinco) dias do ano, no período de vigência contratual.
- k) A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento.
- l) Em momentos de ataques DOS e DDoS, todo tráfego limpo deve ser reinjetado na infraestrutura da contratante através de túneis GRE (Generic Routing Encapsulation), configurado entre a plataforma de DOS e DDoS da contratada e o CPE do contratante.
- m) Para a mitigação dos ataques não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro.
- n) As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, durante os 365 (trezentos e sessenta e cinco) dias do ano, no período de vigência contratual
- o) Em nenhum caso será aceito bloqueio de ataques de DOS e DDoS por ACLs em roteadores de bordas da contratada.
- p) A contratada deve iniciar a mitigação de ataques de DDoS em pelo menos 15 minutos.
- q) Cada alerta deverá ter um número de identificação que facilite sua consulta.
- r) Informar a data de início e fim do acompanhamento do alerta.
- s) Volume de ataques sumarizados por hora, dia, semana e mês.
- t) Relatório por tipos de ataques.
- u) O Portal de monitoração da CONTRATADA deverá possuir uma interface única para acesso às suas funcionalidades, independentemente dos equipamentos ou tecnologias empregadas para a prestação dos serviços.

v) O Portal de Gerência deverá permitir o acesso simultâneo a, pelo menos, um administrador de rede da CONTRATANTE.

27.74. **ESPECIFICAÇÕES NEXT GENERATION FIREWALL - NFGW (POR DEMANDA):**

27.75. A solução NFGW será distribuída em TIPO 1 e TIPO 2 contemplando licença PREMIUM para todos os equipamentos, conforme Tabela a abaixo:

Unidade do IGESDF	QNTD.de NFGW do TIPO 1	QNTD.de NFGW do TIPO 2	LICENÇA
Hospital de Base – HB	2		PREMIUM
Hospital Regional de Santa Maria – HRSM	2		PREMIUM
Hospital Cidade do Sol - HSOL		1	PREMIUM
PO700		1	PREMIUM
SIA		1	PREMIUM
UPA – Ceilândia		1	PREMIUM
UPA - Núcleo Bandeirante		1	PREMIUM
UPA - Recanto das Emas		1	PREMIUM
UPA - São Sebastião		1	PREMIUM
UPA – Samambaia		1	PREMIUM
UPA – Sobradinho		1	PREMIUM
UPA – Brazlândia		1	PREMIUM
UPA – Ceilândia (Setor O)		1	PREMIUM
UPA – Gama		1	PREMIUM
UPA – Paranoá		1	PREMIUM
UPA – Planaltina		1	PREMIUM
UPA – Riacho Fundo II		1	PREMIUM
UPA – Vicente Pires		1	PREMIUM
Unidade do IGESDF Tipo 1 (sob demanda)	1		PREMIUM
Unidade do IGESDF Tipo 2 (sob demanda)	1		PREMIUM
Unidade do IGESDF Tipo 3 (sob demanda)		1	PREMIUM
Unidade do IGESDF Tipo 4 (sob demanda)		1	PREMIUM

Unidade do IGESDF Tipo 5(sob demanda)		1	PREMIUM
--	--	---	---------

27.76. Solução de NFGW Principais (TIPO 1) devem ser compostas deve ser composta por 2 equipamento configurados em Cluster, já a Solução de NFGW Secundaria (TIPO 2) deve ser composta por 1 equipamento.

27.77. DETALHAMENTO TÉCNICO PARA SOLUÇÃO DE NFGW DO TIPO 1: (modelo de referencia Fortigate 401F, modelo atual Fortigate 500E)

27.78. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

27.79. A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO.

27.80. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo.

27.81. Deve possuir e estar licenciado durante a vigência do contrato, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention e contextos virtuais.

27.82. Deve possuir fonte de alimentação com chaveamento automático 110/220V.

27.83. Deve possuir firewall com capacidade mínima de processamento de 79 (setenta e nove) Gbps;

27.84. Deve possuir IPS com capacidade mínima de processamento de 12 (doze) Gbps;

27.85. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 9 (nove) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas, podendo evoluir para até 10 (dez) Gbps durante a vigência do contrato, caso haja necessidade técnica.

27.86. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 3 (tres) Gbps;

27.87. Deve possuir VPN com capacidade de, pelo menos, 50 (cinquenta) Gbps de tráfego IPSec;

27.88. Deve suportar 7.000.000 (sete milhões) conexões simultâneas;

27.89. Deverão ser licenciados para suportar, pelo menos, 5.000 (cinco mil) usuários de VPN SSL.

27.90. Deve suportar, pelo menos, 450.000 (quatrocentos e sessenta mil) novas conexões por segundo;

27.91. Deve suportar, pelo menos, 2.000 (dois mil) túneis de VPN Site-Site.

27.92. Deve suportar, pelo menos, 45.000 (quarenta e cinco mil) túneis de VPN Client- Site;

27.93. Deve possuir, pelo menos, 16 (dezesesseis) interfaces RJ 45.

27.94. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit SFP.

27.95. Deve possuir, pelo menos, 2 (quatro) interfaces 10 Gigabit SFP+.

27.96. Deve incluir licença para a funcionalidade de VPN SSL.

27.97. Deve estar licenciado para 10 (dez) instâncias de firewalls virtuais.

27.98. Deve possuir armazenamento interno mínimo de 2x 480 (quatrocentos e oitenta) Gbps SSD;

27.99. Todos os equipamentos que acompanham a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.

27.100. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

27.101. DETALHAMENTO TÉCNICO PARA SOLUÇÃO DE NFGW DO TIPO2: (modelo de referencia Fortigate 61F, modelo atual não possuímos)

27.102. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

27.103. A solução deve suportar a configuração de cluster de alta disponibilidade no modo ATIVO-ATIVO e ATIVO-PASSIVO.

- 27.104. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo.
- 27.105. Deve possuir e estar licenciado durante a vigência do contrato, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPsec e SSL, Controle de Aplicações, DLP – Data Leak Prevention e contextos virtuais.
- 27.106. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 27.107. Deve possuir firewall com capacidade mínima de processamento de 10 (dez) Gbps.
- 27.108. Deve possuir IPS com capacidade mínima de processamento de 1 (um) Gbps.
- 27.109. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 700 (seiscentos) Mbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.
- 27.110. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 700 (setecentos) Mbps.
- 27.111. Deve possuir VPN com capacidade de, pelo menos, 6 (seis) Gbps de tráfego IPsec.
- 27.112. Deverão ser licenciados para suportar, pelo menos, 200 (duzentos) usuários de VPN SSL.
- 27.113. Deve suportar, pelo menos, 35.000 (trinta e cinco mil) novas conexões por segundo.
- 27.114. Deve suportar, pelo menos, 150 (cento e cinquenta) túneis de VPN Site- Site.
- 27.115. Deve suportar, pelo menos, 500 (quinhentos) túneis de VPN Client-Site.
- 27.116. Deve possuir, pelo menos, 10 (dez) interfaces RJ45.
- 27.117. Deve incluir licença para a funcionalidade de VPN SSL.
- 27.118. Deve estar licenciado para 10 (dez) firewalls virtuais.
- 27.119. Deve possuir armazenamento interno mínimo de 128 (cento e vinte oito) Gbps SSD;
- 27.120. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.
- 27.121. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 27.122. Caso a empresa ganhadora esteja ofertando todos os produtos do lote sendo do mesmo fabricante será permitido a Solução de Gerenciamento e Controle dos itens deste lote, desde que todas as características sejam atendidas;
- 27.123. **REQUISITOS GERAIS DE FUNCIONALIDADES E LICENCIAMENTOS COMUNS para NGFW do TIPO 1 e TIPO 2:**
- 27.124. **FUNCIONALIDADES DE FIREWALL:**
- 27.125. Deve possuir controle de acesso à internet por endereço IP de origem e destino;
- 27.126. Deve possuir controle de acesso à internet por sub-rede;
- 27.127. Deve suportar tags de VLAN (802.1q);
- 27.128. Deve possuir ferramenta de diagnóstico do tipo tcpdump;
- 27.129. Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
- 27.130. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
- 27.131. Deve suportar single-sign-on para Active Directory, RADIUS;
- 27.132. Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
- 27.133. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;
- 27.134. Deve permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
- 27.135. Deve permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;
- 27.136. Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;
- 27.137. Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;
- 27.138. Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- 27.139. Deve suportar aplicações multimídia, como: H.323 e SIP;

- 27.140. Deve possuir tecnologia de firewall do tipo Statefull;
- 27.141. Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
- 27.142. Deve permitir o funcionamento em modo transparente tipo "bridge" sem alterar o endereço MAC do tráfego;
- 27.143. Deve suportar PBR – Policy Based Routing;
- 27.144. Deve permitir a criação de VLANS no padrão IEEE 802.1q;
- 27.145. Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
- 27.146. Deve permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;
- 27.147. Deve permitir forwarding de camada 2 para protocolos não IP;
- 27.148. Deve suportar forwarding multicast;
- 27.149. Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;
- 27.150. Deve permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;
- 27.151. Deve permitir o agrupamento de serviços;
- 27.152. Deve permitir o filtro de pacotes sem a utilização de NAT;
- 27.153. Deve permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- 27.154. Deve possuir mecanismo de anti-spoofing;
- 27.155. Deve permitir criação de regras definidas pelo usuário;
- 27.156. Deve permitir o serviço de autenticação para tráfego HTTP e FTP;
- 27.157. Deve permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;
- 27.158. Deve possuir a funcionalidade de balanceamento e contingência de links;
- 27.159. Deve suportar sFlow;
- 27.160. O dispositivo deve ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas.
- 27.161. Deve ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;
- 27.162. Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
- 27.163. Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;
- 27.164. Deve suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;
- 27.165. Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;
- 27.166. Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 O, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;
- 27.167. Deve suportar SIP, H.323 e SCCP NAT Traversal;
- 27.168. Deve permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;
- 27.169. Deve possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.
- 27.170. **FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO:**
- 27.171. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- 27.172. Deve permitir modificação de valores DSCP para o DiffServ;
- 27.173. Deve permitir priorização de tráfego e suportar ToS;

- 27.174. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;
- 27.175. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- 27.176. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
- 27.177. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- 27.178. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;
- 27.179. Deve controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
- 27.180. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;
- 27.181. **FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY:**
- 27.182. Deve permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;
- 27.183. Deve possuir filtragem de e-mail por palavras chaves;
- 27.184. Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
- 27.185. Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL;
- 27.186. Deve permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;
- 27.187. **FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB:**
- 27.188. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;
- 27.189. Deve possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;
- 27.190. Deve possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;
- 27.191. Deve possuir a funcionalidade de cota de tempo de utilização por categoria;
- 27.192. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo; Webmail; Instituições de saúde; Notícias; Phishing; Hackers; Pornografia; Racismo; Websites pessoais; Compras;
- 27.193. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
- 27.194. Deve permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;
- 27.195. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;
- 27.196. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado;
- 27.197. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
- 27.198. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- 27.199. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
- 27.200. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;
- 27.201. Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;
- 27.202. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;
- 27.203. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);
- 27.204. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;
- 27.205. Deve filtrar o conteúdo baseado em categorias em tempo real;

- 27.206. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;
- 27.207. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- 27.208. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 27.209. Deve permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- 27.210. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;
- 27.211. Deve permitir o bloqueio de redirecionamento HTTP;
- 27.212. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;
- 27.213. Deve possuir Proxy Explícito e Transparente;
- 27.214. Deve implementar roteamento WCCP e ICAP;

27.215. **FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO:**

- 27.216. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
- 27.217. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;
- 27.218. Deve estar orientado à proteção de redes;
- 27.219. Deve permitir funcionar em modo transparente, sniffer e router;
- 27.220. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
- 27.221. Deve permitir a criação de padrões de ataque manualmente;
- 27.222. Deve possuir integração à plataforma de segurança;
- 27.223. Deve possuir capacidade de remontagem de pacotes para identificação de ataques;
- 27.224. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;
- 27.225. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- 27.226. Deve possuir mecanismos de detecção/proteção de ataques;
- 27.227. Deve possuir reconhecimento de padrões;
- 27.228. Deve possuir análise de protocolos;
- 27.229. Deve possuir detecção de anomalias;
- 27.230. Deve possuir detecção de ataques de RPC (Remote Procedure Call);
- 27.231. Deve possuir proteção contra-ataques de Windows ou NetBios;
- 27.232. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);
- 27.233. Deve possuir proteção contra-ataques DNS (Domain Name System);
- 27.234. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;
- 27.235. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);
- 27.236. Deve possuir métodos de notificação de detecção de ataques;
- 27.237. Deve possuir alarmes na console de administração;
- 27.238. Deve possuir alertas via correio eletrônico;
- 27.239. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
- 27.240. Deve ter a capacidade de resposta/logs ativa a ataques;
- 27.241. Deve prover a terminação de sessões via TCP resets;
- 27.242. Deve armazenar os logs de sessões;
- 27.243. Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- 27.244. Deve mitigar os efeitos dos ataques de negação de serviços;
- 27.245. Deve permitir a criação de assinaturas personalizadas;

- 27.246. Deve possuir filtros de ataques por anomalias;
- 27.247. Deve permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- 27.248. Deve permitir filtros de anomalias de protocolos;
- 27.249. Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- 27.250. Deve suportar verificação de ataque na camada de aplicação;
- 27.251. Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;
- 27.252. Deve possuir as seguintes estratégias de bloqueio: pass, drop e reset.
- 27.253. **FUNCIONALIDADE DE VPN:**
- 27.254. Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- 27.255. Deve possuir suporte a certificados PKI X.509 para construção de VPNs;
- 27.256. Deve possuir suporte a VPNs IPSec Site-to-Site e VPNs IPSec Client-to-Site;
- 27.257. Deve possuir suporte a VPN SSL;
- 27.258. Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- 27.259. A VPN SSL Deve possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
- 27.260. Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;
- 27.261. A VPN SSL Deve suportar cliente para plataforma Windows, Linux e Mac OS X;
- 27.262. Deve permitir a arquitetura de VPN hub and spoke;
- 27.263. Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.
- 27.264. **FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES:**
- 27.265. Deve reconhecer, no mínimo, 2.000 (duas mil) aplicações;
- 27.266. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;
- 27.267. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging; Web client; Transferência de arquivos; VoIP;
- 27.268. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- 27.269. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
- 27.270. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- 27.271. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- 27.272. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- 27.273. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- 27.274. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 27.275. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
- 27.276. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
- 27.277. Deve permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;
- 27.278. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;
- 27.279. Deve permitir criação de padrões de aplicação manualmente;
- 27.280. **FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION):**
- 27.281. O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway, deve funcionar de maneira que se consiga que os dados sensíveis não saiam da rede e também Deve funcionar de modo que se

previna que dados não requisitados entrem na sua rede;

- 27.282. Deve inspecionar, no mínimo, os tráfegos de e-mail, HTTP;
- 27.283. Sobre o tráfego de e-mail, deve inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;
- 27.284. Deve realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word;
- 27.285. Deve fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;
- 27.286. Deve aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;
- 27.287. Deve aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;
- 27.288. Deve verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saindes possui um tamanho máximo especificado pelo administrador;
- 27.289. Deve utilizar expressões regulares para composição das regras de verificação dos tráfegos;
- 27.290. Deve tomar minimamente as ações de bloquear, banir usuário e colocar em quarentena a interface sobre as regras que coincidirem com o tráfego esperado pela regra;
- 27.291. Deve permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail, HTTP e mensageiros instantâneos;
- 27.292. Deve permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

27.293. **FUNCIONALIDADE DE BALANCEAMENTO DE CARGA**

- 27.294. Deve permitir a criação de endereços IPs virtuais;
- 27.295. Deve permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;
- 27.296. Deve suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;
- 27.297. Deve permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;
- 27.298. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;
- 27.299. Deve permitir que seja mantido o IP de origem;
- 27.300. Deve suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;
- 27.301. Deve ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;
- 27.302. Deve permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

27.303. **FUNCIONALIDADE DE VIRTUALIZAÇÃO:**

- 27.304. Deve suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;
- 27.305. Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais;
- 27.306. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

27.307. **FUNCIONALIDADE DE SD-WAN**

- 27.308. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 27.309. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.
- 27.310. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.
- 27.311. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.
- 27.312. Solução deve ser capaz de prover Zero Touch provisioning.
- 27.313. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

- 27.314. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.
- 27.315. A solução deve ser capaz de criar VPN "Full-Mesh" em interface gráfica ou CLI, de forma automática, e sem que o administrador precise configurar site por site.
- 27.316. A configuração VPN IPSEC Deve oferecer suporte para DH Group: 14 e 15.
- 27.317. Reconhecimento em camada 7 totalmente segregado da camada 4.
- 27.318. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/range de IPs de destino.
- 27.319. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 27.320. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc).
- 27.321. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a Ipv4 ou Ipv6.
- 27.322. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.
- 27.323. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.
- 27.324. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de saúde melhor que o link atual.
- 27.325. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.
- 27.326. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.
- 27.327. **FUNCIONALIDADE DE GERENCIAMENTO DO NGFW**
- 27.328. A solução deve ser baseada em máquina virtual ou appliance físico do mesmo fabricante da solução de NGFW e SD-WAN, e ter como objetivo gerenciar de modo centralizado todos os equipamentos a partir de uma única console de administração;
- 27.329. Poderá ser entregue em formato de appliance físico ou appliance virtual;
- 27.330. Para appliance virtual, deve ser compatível com VMWare 7.0 e superiores, Hyper-V 2016 e superiores, e KVM. Deverá estar devidamente licenciada para:
- a) Gerenciar, no mínimo, o total de NGFWs/Clusters unidades (NGFW, SD-WAN ou Sistemas Virtuais) dos equipamentos da solução de NGFW e SD-WAN de forma simultânea;
 - b) Não deverá existir limite para o número de vCPUs no appliance virtual;
 - c) Não deverá existir limite para a expansão da memória RAM no appliance virtual;
- 27.331. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
- 27.332. A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
- 27.333. Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;
- 27.334. Permitir acesso concorrente de administradores, permitindo ainda que seja definida uma cadeia de aprovação das alterações realizadas;
- 27.335. Possibilitar a criação e administração de políticas de firewall, controle de aplicação, sistema de prevenção a intrusão (IPS – Intrusion Prevention System), antivírus, filtro de URL e SD-WAN;
- 27.336. Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;
- 27.337. Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;
- 27.338. Permitir usar palavras chaves ou cores para facilitar identificação de regras;

- 27.339. Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;
- 27.340. Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;
- 27.341. Permitir criação de regras que fiquem ativas em horário definido;
- 27.342. Permitir criação de regras com data de expiração;
- 27.343. Realizar o backup das configurações para permitir o retorno de uma configuração salva;
- 27.344. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.
- 27.345. Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas
- 27.346. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
- 27.347. Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota de maneira centralizada;
- 27.348. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;
- 27.349. Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 27.350. Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.
- 27.351. Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;
- 27.352. A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato.
- 27.353. **FUNCIONALIDADE DE GERENCIAMENTO DE LOGS DO NGFW (online e off-line)**
- 27.354. Deve ser do mesmo fornecedor das soluções ofertadas, suportando nativamente todos os recursos listados.
- 27.355. Deve considerar o volume de equipamentos ofertados, considerando todo o licenciamento necessário para a correta gestão dos elementos de rede;
- 27.356. Deve ser fornecido com licenciamento perpétuo, cabendo apenas a renovação de suporte, caso seja de interesse do órgão;
- 27.357. Deve suportar a recepção de 100% dos logs com armazenamento mínimo de 6 (seis) meses consecutivos para cada appliance;
- 27.358. A CONTRATADA deverá no final dos 6 meses entregar o arquivo de Log para CONTRATANTE;
- 27.359. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 27.360. Deve ser fornecido em software que suporte
- 27.361. O sistema deverá suportar contas de usuário/senha estáticas;
- 27.362. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita e acesso de leitura;
- 27.363. O sistema deverá suportar o método de autenticação externo usuário/conta do servidor Radius;
- 27.364. A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC;
- 27.365. Deve possuir integração nativa com Microsoft Teams;
- 27.366. Deve possuir integração via Fluentd, permitindo o streaming de logs para múltiplos destinos;
- 27.367. Essas comunicações deverão ser protegidas e criptografadas;
- 27.368. Deverá permitir que todos os alarmes e eventos sejam registrados na console de Gerência.
- 27.369. Deve permitir a correlação de eventos, provendo dashboards diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;
- 27.370. O portal deve permitir uma visão geral do tráfego de rede e da postura de segurança, incluindo widgets intuitivos com informações como principais países, principais ameaças, principais origens de tráfego, principais destinos, principais aplicativos e hits de políticas, bem como gráficos para mostrar logins de administrador, eventos do sistema, e uso de recursos;
- 27.371. O portal deve suportar a sua configuração possibilite seu uso via multi-tenant, ou seja, com a possibilidade de se criarem vários portais de acesso independentes entre si para fins de administração distribuída;
- 27.372. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

- 27.373. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;
- 27.374. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
- 27.375. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
- 27.376. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
- 27.377. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
- 27.378. Deve possuir mecanismos de remoção automática para logs antigos;
- 27.379. Permitir importação e exportação de relatórios;
- 27.380. Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;
- 27.381. Deve permitir exportar os logs no formato CSV;
- 27.382. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
- 27.383. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
- 27.384. A solução deve ter relatórios predefinidos;
- 27.385. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
- 27.386. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
- 27.387. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
- 27.388. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
- 27.389. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
- 27.390. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
- 27.391. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
- 27.392. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
- 27.393. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
- 27.394. Permitir o envio por e-mail relatórios automaticamente;
- 27.395. Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;
- 27.396. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
- 27.397. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
- 27.398. Deve permitir o uso de filtros nos relatórios;
- 27.399. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
- 27.400. Permitir especificar o idioma dos relatórios criados;
- 27.401. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
- 27.402. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
- 27.403. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
- 27.404. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
- 27.405. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
- 27.406. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
- 27.407. Deve permitir visualizar em tempo real os logs recebidos;
- 27.408. Deve permitir o encaminhamento de log no formato syslog;
- 27.409. Deve permitir o encaminhamento de log no formato CEF (Common Event Format);

- 27.410. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
- 27.411. Deve permitir gerar alertas de eventos a partir de logs recebidos;
- 27.412. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;
- 27.413. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados pelos computadores, atribuição de pontuações de risco que definem os vereditos dos níveis de comprometimento como baixo, médio ou alto;
- 27.414. Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;
- 27.415. Deve suportar recursos de automação (playbooks) que, por meio de integrações com soluções de firewall, endpoint, Email, ITSM e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;
- 27.416. Deve evidenciar o consumo de banda do SD-WAN ao longo do tempo;
- 27.417. Deve mostrar a utilização de banda por interface e aplicação;
- 27.418. Deve mostrar a performance para uma aplicação específica de acordo com a latência, jitter, perda de pacote e banda consumida;
- 27.419. Deve mostrar o MOS (Mean Opinion Score) por interface, bem como a qualidade da chamada de voz;
- 27.420. Deve criar automaticamente um gráfico para cada health check criado na solução de SD-WAN, indicando parâmetros como latência, jitter e perda de pacote de acordo com o tempo selecionado;
- 27.421. Deve mostrar o status do ambiente de SD-WAN para, pelo menos: maiores problemas de rede, aplicações mais usadas, elementos que mais consomem banda e MOS;
- 27.422. Deve possuir relatórios nativos de SD-WAN;
- 27.423. Permitir para reconstruir o banco de dados, gerando relatórios a partir de logs arquivados (offline):
- a) Permitir reimportar os arquivos de log que foram exportados.
 - b) A importação deve acionar automaticamente com a inserção dos logs no banco de dados SQL no gerenciador de logs de produção.
 - c) Sendo possível, em outro gerenciador de logs, se necessário para esta ação, estar licenciado dedicado para esta função, permitir extrair dados de log mais antigos que atendam aos critérios filtrados, evitando assim, a duplicação de logs e a necessidade de alterar repetidamente a Política de Retenção de Logs no Gerenciador de produção.
- 27.424. **Manutenção e suporte Técnico para Solução de SD_WAN (Link de Internet e NFGW):**
- 27.425. Manutenção e Suporte Técnico referente a prestação de serviços de SD-WAN, devem estar de acordo com o especificado neste item.
- 27.426. O suporte e a manutenção deverão ser providos durante toda vigência do contrato.
- 27.427. Deverá monitorar o quantitativo instalado. A CONTRATANTE, deve ter acesso de leitura a planilha de monitoração para fins de acompanhamento e auditoria.
- 27.428. Dentro do contrato, deverá estar incluída a atualização de softwares, drivers e hardware ou novos releases sem custos adicionais a CONTRATANTE.
- 27.429. A CONTRATADA deve emitir relatório sempre que ocorrer atualizações de softwares, driver e hardware ou novos releases sem custos adicionais a CONTRATANTE, contendo:
- a) Descrição do procedimento que será executado;
 - b) Cronograma de Atividades;
 - c) Impacto e eventuais procedimentos de contingência;
 - d) Bem como relatório posterior sobre os resultados obtido.
- 27.430. O Suporte deverá ser prestado com disponibilidade 24 (vinte e quatro) horas por dia, 7 (sete) dias na semana, durante os 365 (trezentos e sessenta e cinco) do ano.
- 27.431. Deverá ser disponibilizado pela CONTRATADA, os meios necessários para que os técnicos especialistas executem suas atividades (equipamentos, ferramentas e transporte) sem ônus para CONTRATANTE.
- 27.432. A CONTRATADA, deverá utilizar a ferramenta de ITSM da CONTRATANTE, para registro de chamados, acompanhamento dos chamados e emissão de relatórios.
- 27.433. Todo chamado deve ser registrado em ITSM próprio da CONTRATANTE, em que haja possibilidade de visualização por parte da CONTRATADA.
- 27.434. Para finalizar os chamados registrados devem ser inseridos os registros das tratativas adotadas.
- 27.435. Todo e qualquer problema detectado nos itens/serviços descritos neste Elemento Técnico, deverão ser, de forma imediata, ser relatados à equipe de Fiscais do CONTRATANTE.

27.436. Todas as mudanças adotadas por iniciativa da CONTRATADA nas configurações, deverão ser efetuadas mediante aprovação do CONTRATANTE, por se tratar de ambiente Hospitalar.

27.437. A CONTRATADA deverá emitir uma declaração prévia, com antecedência mínima de 48 (quarenta e oito) horas, contendo:

- a) Descrição do procedimento que será executado;
- b) Cronograma de Atividades;
- c) Impacto e eventuais procedimentos de contingência;
- d) Bem como relatório posterior sobre os resultados obtido.

27.438. O suporte deverá incluir resposta a chamados críticos em tempo inferior a 60 (sessenta) minutos e permitir a comunicação por meio de e-mail, whatsapp ou telefone (devendo a CONTRATADA fornecer um número telefônico para contato direto da CONTRATANTE com a CONTRATADA). No momento do aceite de cada ordem de serviço, a CONTRATADA deverá comprovar está em operação o suporte técnico descrito neste item.

27.439. Os serviços de Suporte Técnico compreendem todos os chamados relativos aos itens referenciados neste Elemento Técnico, com serviço previamente planejado e executado pela CONTRATADA, bem como todos os chamados que objetivem esclarecer dúvidas na utilização dos serviços prestados diretamente pelo provedor, independentemente de esses serviços terem sido provisionados pela CONTRATADA ou pela CONTRATANTE.

27.440. Os serviços de suporte técnico deverão ser prestados pela CONTRATADA sem qualquer ônus adicional para a CONTRATANTE.

27.441. Os chamados de suporte técnico serão classificados por Criticidade, de acordo com o impacto no ambiente computacional da CONTRATANTE.

27.442. Serão utilizados 3 (três) níveis, com prazo de início do atendimento e prazo para conclusão conforme Tabela 01 – SLA de atendimento.

27.443. Criticidade Alta - Deveremos entender como criticidade ALTA um serviço totalmente fora de operação, com SLA de 20 minutos para captura de chamado e início de atendimento, e até 04 horas para resolução do problema.

27.444. Criticidade Média - Deveremos entender como Severidade Média incidentes que não impeçam o uso do equipamento, serviços e/ou consultas em geral, com SLA de 20 minutos para captura de chamado e início de atendimento e até 06 horas para resolução do problema;

27.445. Criticidade Baixa - Deveremos entender como Severidade Baixa os testes funcionais e consultas gerais do equipamento, com SLA de 20 minutos para captura de chamado e início de atendimento e até 08 horas para resolução do problema.

27.446. Para fins de verificação do atendimento, os chamados serão agrupados por nível de severidade e seus prazos de atendimento serão contabilizados mensalmente, conforme Tabela 01 – SLA de atendimento:

Criticidade	Descrição	Prazo para início do atendimento	Prazo para conclusão do atendimento	Desconto por não atendimento no prazo
Alta	Deveremos entender como criticidade ALTA um serviço totalmente fora de operação	20 minutos para captura de chamado	Até 04 horas para resolução do problema	1,5%
Média	Deveremos entender como Severidade Média incidentes que não impeçam o uso do equipamento, serviços e/ou consultas em geral	20 minutos para captura de chamado	Até 06 horas para resolução do problema	1,0%

Baixa	Deveremos entender como Severidade Baixa os testes funcionais e consultas gerais do equipamento	20 minutos para captura de chamado	Até 08 horas para resolução do problema	0,5%
Observação	Troca de equipamentos	30 minutos após abertura do chamado	A CONTRATADA deverá providenciar equipamento reserva de falhas e este equipamento deverá estar disponível em até 1 (um) dia corridos. Obs: Podendo ser negociado com a Gestão	2,0% por dia em atraso

27.447. **Obrigações da Contratada:**

27.448. A CONTRATADA de prestar os serviços com pessoal adequadamente qualificado e capacitado para suas atividades.

27.449. Cumprir rigorosamente todas as programações e atividades do objeto do contrato.

27.450. Prestar os serviços de acordo com o especificado neste instrumento.

27.451. Levar imediatamente ao conhecimento da Fiscalização qualquer fato extraordinário ou anormal que ocorra durante a execução dos serviços a fim de que sejam adotadas medidas cabíveis, bem como comunicar por escrito e de forma detalhada todo tipo de incidente que venha a ocorrer.

27.452. Prestar todos os esclarecimentos que forem solicitados pela Fiscalização, atendendo de imediato as solicitações.

27.453. Responder pelos danos causados ao IGESDF ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços.

27.454. Arcar com despesas decorrentes de infrações relacionadas ao disposto no objeto deste instrumento, durante o desempenho das funções, ainda que fora das dependências do IGESDF.

27.455. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica, normas e legislação. Garantir a supervisão permanente dos serviços de forma a obter uma operação correta e eficaz.

27.456. Manter suporte inerente aos serviços a serem executados, garantindo um serviço de alto padrão, sem nenhum custo adicional para o IGESDF.

27.457. Atender prontamente quaisquer exigências do representante do IGESDF inerentes ao objeto do Contrato.

27.458. Fornecer, na forma solicitada pelo IGESDF, o demonstrativo de utilização dos serviços, objeto do Contrato.

27.459. Comunicar ao IGESDF, por escrito, qualquer anormalidade, sobretudo de caráter urgente, e prestar os esclarecimentos julgados necessários.

27.460. Manter, durante toda a execução do Contrato, em compatibilidade com as obrigações a serem assumidas, todas as condições de qualificação exigidas na contratação, inclusive por meio da atualização dos seus profissionais.

27.461. Indicar um preposto para acompanhar a execução do contrato e responder perante o CONTRATANTE.

27.462. A CONTRATADA deve manter Matriz, Filial ou Escritório de Representação no Distrito Federal, durante toda a vigência do Contrato, com condições adequadas para gerenciar a prestação dos serviços, com linha telefônica, em virtude da necessidade do IGESDF manter contato com o preposto indicado pela empresa.

27.463. CONTRATADA deve fornecer, no ato da assinatura contratual, endereço da matriz, filial ou escritório no Distrito Federal, bem como número de telefone comercial fixo, móvel, fax, também no Distrito Federal, e endereço eletrônico (e-mail), devendo atualizar todos os dados sempre que houver alterações.

27.464. Dar cumprimento a todas as determinações e especificações estabelecidas neste instrumento e assumir inteira responsabilidade pela execução dos serviços contratados, nos termos da legislação vigente.

27.465. Manter arquivo com toda a documentação relativa à execução do contrato.

27.466. A contratada se obriga a manter o fornecimento de bens e serviços, nas mesmas condições estabelecidas neste Elemento Técnico e no preço pactuado, caso exista risco a vida dos pacientes, por, no mínimo, 90 dias ou até a celebração de contrato com outro fornecedor.

28. ANEXO II – DO ELEMENTO TÉCNICO - PROPOSTA

Ao XXXXXXXXXXXX de XXXXXX do XXXXXX

A empresa _____ (razão social), inscrita no CNPJ sob o número _____, inscrição estadual número _____, sediada no endereço (citar endereço completo), para fins de participação no presente processo Seleção de Fornecedores n.º _____, vem pela presente apresentar - em anexo - sua proposta de preços, de acordo com as exigências do Ato Convocatório supracitado.

Unidade do IGESDF	Velocidade mínima do Link de Internet	QNTD.de NFGW do TIPO 1	QNTD.de NFGW do TIPO 2	LICENÇA	Valor Unitário	Valor Mensal	Valor Global para 30 meses
Hospital de Base – HB	1Gbps	2		PREMIUM	R\$	R\$	R\$
Hospital Regional de Santa Maria – HRSM	1Gbps	2		PREMIUM	R\$	R\$	R\$
Hospital Cidade do Sol - HSOL	300 Mbps		1	PREMIUM	R\$	R\$	R\$
PO700	300 Mbps		1	PREMIUM	R\$	R\$	R\$
SIA	300 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA – Ceilândia	100 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA - Núcleo Bandeirante	100 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA - Recanto das Emas	100 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA - São Sebastião	100 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA – Samambaia	100 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA – Sobradinho	100 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA – Brazlândia	100 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA – Ceilândia (Setor O)	100 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA – Gama	100 Mbps		1	PREMIUM	R\$	R\$	R\$

UPA – Paranoá	100 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA – Planaltina	100 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA – Riacho Fundo II	100 Mbps		1	PREMIUM	R\$	R\$	R\$
UPA – Vicente Pires	100 Mbps		1	PREMIUM	R\$	R\$	R\$
Unidade do IGESDF Tipo 1 (sob demanda)	2 Gbps	1		PREMIUM	R\$	R\$	R\$
Unidade do IGESDF Tipo 2 (sob demanda)	1 Gbps	1		PREMIUM	R\$	R\$	R\$
Unidade do IGESDF Tipo 3 (sob demanda)	600 Mbps		1	PREMIUM	R\$	R\$	R\$
Unidade do IGESDF Tipo 4 (sob demanda)	300 Mbps		1	PREMIUM	R\$	R\$	R\$
Unidade do IGESDF Tipo 5 (sob demanda)	100 Mbps		1	PREMIUM	R\$	R\$	R\$

Valor Global da proposta para o período de 30 meses: R\$ _____

1. Prazo de validade da proposta é de 90 (noventa) dias corridos, contados a partir da sua assinatura.
2. Declaramos estar cientes de todas as cláusulas do instrumento convocatório, bem como de seus anexos.
3. Apresentamos, conforme exigido no Ato Convocatório, os dados bancários para pagamento mediante depósito bancário em conta corrente, constando:

Nome e número do Banco:

Agência:

Número da conta concorrente:

4. Declaramos que nos preços cotados estão incluídas todas as despesas, tais como tributos, seguros, transporte, pagamento de mão de obra, treinamento, frete até o destino, seguros, garantia e todos os demais encargos e/ou descontos porventura existentes.

Local/data

(Assinatura do responsável pela empresa) Nome/Cargo

29. ANEXO III – DO ELEMENTO TÉCNICO - ORDEM DE FORNECIMENTO

29.1. Solicitamos à Empresa _____, fornecer os itens especificados abaixo nos locais especificados, em conformidade com o objeto, Anexo III do Contrato Nº _____ - IGESDF

Unidade do IGESDF	Velocidade mínima do Link de Internet	QNTD.de NFGW do TIPO 1	QNTD.de NFGW do TIPO 2	LICENÇA
Hospital de Base – HB				
Hospital Regional de Santa Maria – HRSM				
Hospital Cidade do Sol - HSOL				
PO700				
SIA				
UPA – Ceilândia				
UPA - Núcleo Bandeirante				
UPA - Recanto das Emas				
UPA - São Sebastião				
UPA – Samambaia				
UPA – Sobradinho				
UPA – Brazlândia				
UPA – Ceilândia (Setor O)				
UPA – Gama				
UPA – Paranoá				
UPA – Planaltina				
UPA – Riacho Fundo II				
UPA – Vicente Pires				
Unidade do IGESDF Tipo 1 (sob demanda)				
Unidade do IGESDF Tipo 2 (sob demanda)				
Unidade do IGESDF Tipo 3 (sob demanda)				
Unidade do IGESDF Tipo 4 (sob demanda)				
Unidade do IGESDF Tipo 5(sob demanda)				

Local de entrega: _____

Brasília, ____ de _____ de 20__.

NOME:
Cargo:
Matrícula:

30. ANEXO V – DO ELEMENTO TÉCNICO - ENDEREÇO IGESDF

30.1.

UNIDADES	ENDEREÇO	CEP
Hospital de Base – HB	SMHS - Área Especial, Q. 101 - Asa Sul, Brasília - DF	70.330-150
Hospital Regional de Santa Maria – HRSM	Quadra AC 102, Conj. A, B, C e D, s/nº – Santa Maria/DF	72.502-100
Hospital Cidade do Sol - HSOL	St. N QNN 27 - Ceilândia, Brasília - DF	72225-270
PO700	Edifício PO 700 - Setor de Rádio e Televisão Norte (SRTVN) - Quadra 701 - Lote D - 3º andar - Asa Norte - Brasília/DF	70.719-040
SIA	SIA, Trecho 17, Rua 06, Lote 115	70.297-400
UPA Brazlândia	Vila São José, Q 37, AE1, Posto de Saúde	72.745-000
UPA Ceilândia	Área Especial D, Via P1 Norte - Ceilândia, Brasília - DF,	72.225-270
UPA Ceilândia II	Expansão do St. O QNO 23 - Ceilândia	72.262-104
UPA Gama	Setor de Indústria QI 7, Área Reservada 2	72.445-070
UPA Núcleo Bandeirante	DF – 075 KM 180, Área Especial EPNB	71.732-010
UPA Paranoá	Paranoá Parque Q 1/2 Comercial 1 AE 4 EPC	71.587-032
UPA Planaltina	Setor Habitacional Mestre D'Armas, Q 23 MD 2 Lote 1	73.402-006
UPA Recanto das Emas	Q. 102 – Área Especial 1 – Avenida Recanto	72.600-228
UPA Riacho Fundo	QN 31 Conjunto 3 Lote 1	71.880-713
UPA Samambaia	QS 107, Conjunto 4, Área Especial – Samambaia Sul.	72.322-700
UPA São Sebastião	QD 102 conj. 1 LT 1, Residencial Oeste, São Sebastião	71.692-101

UPA Sobradinho	DF-420, em frente à AR-13, próximo ao COER	73.080-050
UPA Vicente Pires	Rua 10 QD 4D Chácara 135	70.297-400

31. ANEXO II AO EDITAL 034/2024 - MODELO DE DECLARAÇÃO DE NÃO VÍNCULO

TIMBRE DA EMPRESA
NOME COMPLETO DA EMPRESA
CNPJ N°

Ao Instituto de Gestão Estratégica de Saúde do Distrito Federal - IGESDF

Objeto: xxxxxxxxxxxxxx

A Empresa XXXXXXXXXXXXXXXXXXXXXXXX, inscrita sob CNPJ nº XX.XXX.XXXX/XXXX-XX, por meio do seu representante legal o Sr(a).: _____, CPF nº XXXXXXXXXXXX-X, RG nº XXXXXXXX SSP/XX, declara, para os fins de cumprimento ao disposto no item 4 DAS CONDIÇÕES PARA PARTICIPAÇÃO do Edital, que em seu quadro de funcionários não há empregados e/ ou sócios que se enquadram nas vedações previstas nas referidas condições para participação.

Brasília/DF ___ de _____ de 202X.

NOME DO REPRESENTANTE LEGAL
CPF
NOME DA EMPRESA

Obs.: a declaração deverá estar assinada pelo representante legal de forma manual ou digitalmente (por token).

32. ANEXO III AO EDITAL 034/2024 - MODELO DE DECLARAÇÃO DE PREÇO

TIMBRE DA EMPRESA
NOME COMPLETO DA EMPRESA
CNPJ N°

Ao Instituto de Gestão Estratégica de Saúde do Distrito Federal - IGESDF

A empresa _____, CNPJ nº _____, endereço completo: _____, informa que não poderá encaminhar cópias de 03 (três) notas fiscais emitidas a no máximo 90 (noventa) dias ou contratos vigentes com outras empresas pelo seguinte motivo: detalhar os motivos pelos quais a empresa não pode apresentar notas fiscais. Diante disso, declaramos sob as penas do Art. 299 do Código Penal que os preços praticados junto ao INSTITUTO DE GESTÃO ESTRATÉGICA DE SAÚDE DO DISTRITO FEDERAL (IGESDF) - CNPJ: 28.481.233/0001-7, são os praticados com outros contratantes e os de mercado, não havendo majoração.

Brasília/DF ___ de _____ de 202X.

NOME DO REPRESENTANTE LEGAL
CPF
NOME DA EMPRESA

Obs.: a declaração deverá estar assinada pelo representante legal de forma manual ou digitalmente (por token).



Documento assinado eletronicamente por **KATIA LUCIA BARROS - Matr.0001583-9, Gerente-Corporativo(a)**, em 31/07/2024, às 10:28, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



Documento assinado eletronicamente por **THALES MARINHO TEIXEIRA - Matr.0000467-0, Chefe de Núcleo - Corporativo**, em 31/07/2024, às 17:12, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



Documento assinado eletronicamente por **MAICON DOUGLAS AMARAL DO NASCIMENTO - Matr.0001878-7, Analista II**, em 01/08/2024, às 07:53, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



A autenticidade do documento pode ser conferida no site:
http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0
verificador= **147209089** código CRC= **B020D619**.

"Brasília - Patrimônio Cultural da Humanidade"
SMHS - Área Especial - Quadra 101 - Bairro Asa Sul - CEP 70335900 - DF

04016-00030943/2024-24

Doc. SEI/GDF 147209089

Criado por **00018787**, versão 10 por **00004670** em 31/07/2024 09:22:27.