EDITAL DO PREGÃO ELETRÔNICO Nº 04/2015

O Distrito Federal, por meio da Procuradoria-Geral do Distrito Federal – PGDF, leva ao conhecimento dos interessados que fará realizar licitação, na modalidade Pregão, na forma Eletrônica, mediante as condições estabelecidas neste Edital, de acordo com o regulamento da Lei n.º 10.520/2002, Decreto Federal n.º 5.450/2005, Decretos Distritais nº 23.460/2002, 25.966/2005, 26.851/2006, 32.985/2011 e, subsidiariamente, pela Lei n.º 8.666/1993 e alterações subsequentes, observando a Lei Complementar n.º 123/2006, Decreto Federal nº 7.174/2010 que foi recepcionado pelo Decreto Distrital 34.637/2013, além de outras normas aplicáveis ao objeto deste certame.

A Sessão Pública do Pregão Eletrônico será conduzida por servidor, designado Pregoeiro, mediante o Decreto de 17 de junho de 2013, publicada no DODF nº 125, de 18 de junho de 2013, e, será realizada por meio de Sistema Eletrônico COMPRASNET, conforme a indicação abaixo:

PROCESSO Nº. : 020.003.077/2013
TIPO DE LICITAÇÃO: Menor Preço
REGIME DE EXECUÇÃO: Empreitada por preço global
NOVA DATA DE ABERTURA: 29/09/2015
HORÁRIO: 09h30min (nove horas e trinta minutos horário de Brasília/DF
ENDEREÇO ELETRÔNICO: www.comprasnet.gov.br
CÓDIGO UASG: 926121

I - DO OBJETO

Contratação de empresa para fornecimento de solução de segurança de rede, composta por 6 (seis) *firewalls appliances*, sistema de gerencia e monitoração centralizada, serviços de instalação e configuração, transferência de conhecimento, garantia e suporte técnico on-site, de acordo com as especificações e condições descritas no Termo de Referência que integra o Anexo I e demais anexos deste Edital.

II – DA SOLICITAÇÃO DE ESCLARECIMENTOS E DA IMPUGNAÇÃO AO EDITAL

2.1.Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao pregoeiro, até três dias úteis anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico, no endereço eletrônico **licitacao@pg.df.gov.br**

2.2.Até dois dias úteis antes da data fixada para abertura da sessão pública, qualquer pessoa poderá impugnar o ato convocatório deste pregão, na forma eletrônica, pelo endereço eletrônico **licitacao@pg.df.gov.br**.

2.3. Caberá ao pregoeiro, auxiliado pelo setor responsável pela elaboração do Termo de Referência, parte integrante do edital, decidir sobre a impugnação no prazo de até vinte e quatro horas e, neste mesmo prazo prestar os esclarecimentos requeridos.

2.4. Acolhida a impugnação contra este Edital ou se, por qualquer motivo, houver mudança em seus termos, será providenciada nova publicação, com designação de nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

2.5. As respostas às impugnações e aos esclarecimentos solicitados serão disponibilizadas no sistema eletrônico para os interessados.

III - DA PARTICIPAÇÃO NA LICITAÇÃO

3.1. Poderão participar deste Pregão:

3.1.1. empresário individual e sociedade empresária, do ramo de atividade do objeto desta licitação, que atenda a todas as condições estabelecidas neste Edital e seus Anexos; e

3.1.2. que esteja credenciado perante o sistema eletrônico provido pela Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI), por meio do sítio www.comprasnet.gov.br.

3.2. Não poderão participar deste Pregão**:**

3.2.1. sociedades integrantes de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum, exceto se demonstrado que não agem representando interesse econômico em comum;

3.2.2. empresário individual ou sociedade empresária, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou termo de referência ou projeto executivo ou o qual ou da qual o autor do projeto seja dirigente, gerente, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto ou controlador, responsável técnico ou subcontratado

3.2.3. empresário individual ou sociedade empresária declarado(a) inidôneo(a) para licitar ou contratar com a Administração Pública, direta ou indireta, Federal, Estadual, Municipal e Distrital, bem como o que esteja punido com suspensão do direito de licitar ou contratar em qualquer esfera da Federação, em qualquer dos Poderes;

3.2.4. sociedade estrangeira não autorizada a funcionar no País;

3.2.5. empresário individual ou sociedade empresária que se encontre em processo de dissolução, recuperação judicial ou extrajudicial, falência, concordata, concurso de credores, liquidação, fusão, cisão, ou incorporação;

3.2.6. consórcio de empresas, qualquer que seja sua forma de constituição e pessoas físicas não empresárias.

3.2.7. empresário individual ou sociedade empresária, que tenha proprietário, administrador, ou sócio com poder de direção que seja familiar de agente público, preste serviços ou desenvolva projeto no órgão ou entidade da Administração Pública do Distrito Federal em que este exerça cargo em comissão ou função de confiança, na forma prescrita pelo Decreto Distrital. nº 32.751/2011.

3.2.7.1. entende-se por familiar o cônjuge, companheiro (a) ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau, inclusive.

3.2.7.2. as vedações deste item estendem-se às relações homoafetivas

3.2.8. direta ou indiretamente o servidor ou dirigente da Procuradoria-Geral do Distrito Federal.

3.2.8.1. considera-se participação indireta a existência de qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista do autor do termo de referência ou projeto, pessoa física ou jurídica e do pregoeiro e de sua equipe de apoio com a licitante ou responsável pelo fornecimento de bens e serviços a estes necessários.

IV – DO CREDENCIAMENTO

4.1. Os interessados em participar deste Pregão deverão credenciar-se, previamente, perante o sistema eletrônico provido pela Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI), por meio do sítio www.comprasnet.gov.br.

4.2. Para ter acesso ao sistema eletrônico, os interessados deverão dispor de chave de identificação e senha pessoal, obtidas junto à SLTI, onde também deverão informar-se a respeito do seu funcionamento e regulamento e receber instruções detalhadas para sua correta utilização.

4.3. O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação por ela efetuada diretamente, ou por seu representante, não cabendo ao provedor do sistema ou a PGDF responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

4.4. O credenciamento junto ao provedor do sistema implica a responsabilidade legal da licitante e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão na forma eletrônica.

4.5. Caberá a licitante comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a inviabilidade do uso da senha, para imediato bloqueio de acesso.

V – DA PROPOSTA ELETRÔNICA

5.1. A licitante deverá encaminhar proposta, exclusivamente por meio do sistema eletrônico, até a data e horário, marcados para abertura da sessão, quando então encerrar-se-á automaticamente a fase de recebimento de propostas, **devendo declarar em campo próprio no sistema**:

5.1.1. o **valor global do item cotado**, sobre **o qual incidirão os lances**, **compreendendo a soma do valor total dos seus subitens descritos no Termo de Referência**, em algarismo, já considerados e inclusos, todos os custos necessários tais como impostos, taxas, tributos e quaisquer outras despesas que incidam ou venham a incidir sobre o objeto do item ofertado;

5.1.2. a **descrição dos produtos/serviços que compõem o item ofertado,** e em caso de discordância existente entre as especificações do objeto descritas no Comprasnet e as constantes deste edital, prevalecerão as últimas;

5.1.3. que **cumpre plenamente** os requisitos de habilitação e que sua proposta está em conformidade com as exigências deste edital.

5.1.4. para fins do disposto no inciso V do art. 27 da Lei nº 8.666, de 21 de junho de 1993, acrescido pela Lei nº 9.854, de 27 de outubro de 1999, **que não emprega menor** de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor, a partir de 14 (quatorze) anos, na condição de aprendiz, nos termos do inciso XXXIII, do art. 7º da Constituição Federal.

5.1.5. quando enquadrada como microempresa ou empresa de pequeno porte, **que cumpre os requisitos legais para a respectiva qualificação** e que está apta a usufruir do tratamento favorecido, nas condições do Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, instituído pela Lei Complementar nº. 123, de 14 de dezembro de 2006, em especial quanto ao seu art. 3º, e que não se enquadra nas situações relacionadas no §4º do referido artigo.

5.1.6. **que cumpre os requisitos** estabelecidos no art. 5º do Decreto nº 7.174, de 2010, caso pretenda exercer o direito de preferência disposto no mencionado Decreto e disponha da documentação comprobatória para tal fim, prevista neste edital.

5.2. As licitantes arcarão com todos os custos decorrentes da elaboração e apresentação de suas propostas.

5.3. O preço oferecido deve ser expresso em real e estar compatível com os praticados no mercado.

5.4.O valor da proposta será fixo e irreajustável.

5.5. A declaração falsa relativa ao cumprimento dos requisitos previstos nesta licitação sujeitará a licitante às sanções estabelecidas neste edital.

5.6. A licitante deverá obedecer aos termos deste Edital e seus Anexos, assim como a proposta apresentada deverá atender a todas as especificações e condições estabelecidas.

5.7. As propostas ficarão disponíveis no sistema eletrônico.

5.8. Qualquer elemento que possa identificar a licitante importa desclassificação da proposta, sem prejuízo das sanções previstas nesse edital.

5.9. Até a abertura da sessão, a licitante poderá retirar ou substituir a proposta anteriormente encaminhada.

5.10. Depois da abertura da sessão não serão admitidas alterações nas propostas apresentadas, ressalvadas apenas a redução do preço proposto e aquelas alterações destinadas a sanar evidentes erros formais.

5.11. Decorrido o prazo de validade das propostas, sem convocação para contratação, ficam as licitantes liberadas dos compromissos assumidos.

5.12. A apresentação da proposta implica plena aceitação, pela licitante, das condições estabelecidas neste Edital e seus Anexos.

VI – DA ABERTURA DA SESSÃO PÚBLICA

6.1 No dia e horário, indicados no preâmbulo deste Edital, no sítio www.comprasnet.gov.br, será realizada a abertura da sessão pública deste Pregão, conduzida pela Pregoeira.

6.2. Durante a sessão, a comunicação entre a Pregoeira e as licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico.

6.3. Incumbirá à Licitante acompanhar as operações no Sistema Eletrônico durante a sessão pública do Pregão Eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo Sistema ou de sua desconexão.

6.4. A Licitante será responsável por todas as transações que forem efetuadas em seu nome no Sistema Eletrônico, assumindo como firmes e verdadeiras sua proposta de preços e lances inseridos em sessão pública.

VII – DA CLASSIFICAÇÃO DAS PROPOSTAS

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

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

VIII – DA FORMULAÇÃO DE LANCES

8.1. Iniciada a fase competitiva, as licitantes que tiveram suas propostas classificadas poderão encaminhar lances sucessivos, exclusivamente por meio do sistema eletrônico e serão imediatamente informadas do recebimento e do valor consignado no registro de cada lance.

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

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

8.4. Em caso de empate, prevalecerá o lance recebido e registrado primeiro.

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

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

8.7. No caso de desconexão do pregoeiro, no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível às licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

8.8. Quando a desconexão do Pregoeiro persistir por tempo superior a dez minutos, a sessão do Pregão será suspensa automaticamente e terá reinício somente após comunicação expressa aos participantes no sítio www.comprasnet.gov.br.

8.9. O encerramento da etapa de lances será decidido pelo Pregoeiro, que informará, com antecedência de 1 a 60 minutos, o prazo para início do tempo de iminência.

8.10. Decorrido o prazo fixado pelo Pregoeiro, o sistema eletrônico encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado pelo sistema, findo o qual será automaticamente encerrada a fase de lances.

8.11. Será assegurada, como critério de desempate, **a preferência de contração para as microempresas e empresas de pequeno porte, nos termos da Lei Complementar nº 123/2006**

8.11.2.Ultrapassada a fase de lances, se a proposta mais bem classificada não tiver sido apresentada por microempresa ou empresa de pequeno porte, e houver proposta de microempresa ou empresa de pequeno porte, na situação de empate, assim considerada(s) aquela(s) que seja(m) iguais ou até 5% (cinco por cento) superiore(s) à proposta mais bem classificada, proceder-se-á da seguinte forma:

8.11.2.1.A microempresa ou a empresa de pequeno porte mais bem classificada poderá apresentar proposta de preço inferior à da licitante mais bem classificada, no prazo de 5 (cinco) minutos, e, se atendidas as exigências deste edital, será adjudicado em seu favor o objeto licitado.

8.11.2.2. Não sendo contratada a microempresa ou empresa de pequeno porte mais bem classificada, na forma do subitem anterior, e havendo outras licitantes que porventura se enquadrem na condição de empate, estas serão convocadas, na ordem classificatória, para o exercício do mesmo direito.

8.11.2.3. A convocada que não apresentar proposta dentro do prazo de 5 (cinco) minutos, controlados pelo Sistema, decairá do direito previsto nos arts. 44 e 45 da Lei Complementar nº 123/2006.

8.11.2.4. Na hipótese de não-contratação nos termos previstos neste item, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame.

8.12. **Por força do que dispõe** o art. 3º da Lei nº 8.248, de 1991 e do Decreto Distrital nº 34.637/2013 que recepcionou o Decreto Federal nº 7.174/2010, **será assegurada a preferência na contratação**, para **fornecedores de bens e serviços de informática e automação**.

8.12.1. O exercício para o direito de preferência disposto neste item será concedido depois do encerramento da fase de lances e após, quando for o caso, da etapa automática de convocação das microempresas ou empresas de pequeno porte, de que trata o item 8.11.

8.12.2. **A licitante que declarar no sistema**, **quando do cadastro de sua proposta**, que atende aos requisitos estabelecidos no art. 5º do Decreto nº 7.174, de 2010, **devendo para tanto dispor da documentação** comprobatória, **será convocada pelo sistema Comprasnet** a exercer o seu direito de preferência, observada a **seguinte ordem de classificação**, na forma definida pelo Poder Executivo Federal:

I - bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB);

II - bens e serviços com tecnologia desenvolvida no País; e

III - bens e serviços produzidos de acordo com o PPB.

8.12.2.1. As microempresas e empresas de pequeno porte que atendam ao disposto nos incisos acima terão prioridade no exercício do direito de preferência em relação às médias e grandes empresas enquadradas no mesmo inciso.

8.12.3. Aplicar-se-ão as regras de preferência previstas neste item com a classificação das licitantes cujas propostas finais estejam situadas até 10% (dez por cento) acima da melhor proposta válida, conforme o critério de julgamento, para a comprovação e o exercício do direito de preferência.

8.12.3.1. serão convocadas as licitantes classificadas que estejam enquadradas nas condições previstas **no subitem 8.12.2 deste Edital**, seguindo a **ordem de classificação**, para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarada vencedora do certame.

8.12.4. Consideram-se bens e serviços de informática e automação com tecnologia desenvolvida no País aqueles cujo efetivo desenvolvimento local seja comprovado junto ao Ministério da Ciência e Tecnologia, na forma por este regulamentada.

8.12.5. A comprovação do atendimento ao PPB dos bens de informática e automação ofertados será feita mediante apresentação do documento comprobatório da habilitação à fruição dos incentivos fiscais regulamentados pelo Decreto 5.906, de 2006, ou pelo Decreto 6.008, de 2006.

8.12.5.1. A comprovação será feita:

8.12.5.1.1**.** eletronicamente, por meio de consulta ao sítio eletrônico oficial do Ministério da Ciência e Tecnologia ou da Superintendência da Zona Franca de Manaus – SUFRAMA; ou

8.12.5.1.2**.** por documento expedido para esta finalidade pelo Ministério da Ciência e Tecnologia ou pela SUFRAMA, mediante solicitação da licitante.

8.12.6**.** A licitante deverá encaminhar **juntamente com a proposta e documentação o(s) certificado(s) comprobatório(s)** do atendimento da habilitação para usufruir o benefício da preferência na contratação, para o qual se declarou apta, estabelecido no art. 5º do Decreto nº 7.174, de 2010 para exame consoante previsto no item 10.3 deste edital.

8.12.7. Caso nenhuma empresa classificada venha a exercer o direito de preferência, seja **por ter deixado de se manifestar no sistema Comprasnet quando do cadastro de sua proposta,** seja **por não ter comprovado o preenchimento** dos requisitos **por meio da documentação comprobatória** estabelecida no art. 7º do Decreto nº 7.174, de 2010, relacionada acima, será declarada vencedora do certame a licitante detentora da proposta mais bem

classificada, antes da concessão da preferência na contratação, para fornecedores de bens e serviços de informática e automação.

IX - DA NEGOCIAÇÃO

9.1. Após o encerramento da etapa de lances, o Pregoeiro poderá encaminhar contraproposta à licitante que tenha apresentado o lance mais vantajoso, observado o critério de julgamento e o valor estimado para a contratação.

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

X - DA ACEITABILIDADE DA PROPOSTA

10.1. A licitante classificada em primeiro lugar deverá encaminhar, no prazo de **3 (três) horas**, contados da solicitação do Pregoeiro, por meio da opção "Enviar Anexo" do sistema Comprasnet, a proposta de preços adequada ao último lance ou valor negociado e demais documentos e comprovações solicitados em Anexo, preferencialmente em arquivo único.

10.1.1. Os originais ou cópias autenticadas da proposta inserida no sistema e da documentação exigida no Edital, deverão ser encaminhados em envelope fechado e identificado o nº do pregão, no prazo máximo de 03 (três) dias úteis, contados a partir da declaração dos vencedores no sistema, ao protocolo da Procuradoria-Geral do Distrito Federal – PGDF, localizada no Setor de Administração Municipal – SAM- Bloco I, térreo, Brasília/DF, CEP: 70620-000, Telefone: (61) 3342-1086.

10.1.2. A **proposta a ser anexada** por meio da opção "Enviar Anexo" do Sistema Comprasnet e **encaminhada** no envelope **deverá conter:**

a) **nome da proponente** e de seu representante legal, endereço completo, telefone, números do CNPJ;

b) o **valor unitário e total** para cada subitem**,** bem como o **valor global do item cotado, de acordo com o modelo constante do anexo II deste edital**, em algarismo, em moeda nacional, já considerados e inclusos todos os custos necessários tais como impostos, taxas, tributos e quaisquer outras despesas que incidam ou venham a incidir sobre o objeto ofertado;

c) a **descrição dos produtos/serviços ofertados, que compõem o item,** de forma a demonstrar o atendimento das especificações estabelecidas no termo de referência constante do **anexo I e I.1,** de acordo com o modelo de proposta constante do **Anexo III** deste edital, e, em caso de discordância existente entre as especificações do objeto descritas no Comprasnet e as constantes deste edital, prevalecerão as últimas;

d) em anexo, **toda documentação necessária** para subsidiar o julgamento técnico da solução ofertada quanto ao atendimento das funcionalidades descritas no Termo de Referência, Anexo I e I.1 deste Edital.

e) a comprovação ponto a ponto, por escrito, por meio de documentação oficial do fabricante, do atendimento às especificações mínimas dos produtos, dos seguintes itens/tópicos contidos no Anexo I.1: 1.6.1.1 a 1.6.1.3, 1.6.1.6, 1.6.1.12, 1.6.1.18 a 1.6.1.22, 1.6.2.2, 1.6.2.4, 1.6.2.5, 1.6.2.8 a 1.6.2.12, 1.6.3.1.1 a 1.6.3.1.22, 1.6.4.1, 1.6.4.3, 1.6.4.5, 1.6.4.8, 1.6.4.12 a 1.6.4.19, 1.6.4.22 a 1.6.4.32, 1.6.5.2 a 1.6.5.8, 1.6.5.10, 1.6.5.12 a 1.6.5.14, 1.6.6.1.2 a 1.6.6.1.11, 1.6.7.1 a 1.6.7.6, 1.6.8.1 a 1.6.8.7, 1.6.9.1 a 1.6.9.7, 1.6.10.1, 1.6.11.1 a 1.6.11.9, 1.6.12.1, 1.6.12.3, 1.6.12.5 a 1.6.12.11, 1.6.12.13, 1.6.12.15 a 1.6.12.18, 1.7.1.1, 1.7.1.2, 1.7.1.6 a 1.7.1.9, 1.7.2.1, 1.7.2.4, 1.7.2.5 a 1.7.2.10, 1.7.2.12 a 1.7.2.21, 1.7.3.1 a 1.7.3.11, 1.7.4.1.3 a 1.7.4.1.10, 1.7.4.1.12, 1.7.4.1.16, 1.7.4.1.19 a 1.7.4.1.21, 1.7.5.1 a 1.7.5.6, 1.7.6.1, 1.7.6.3, 1.7.6.10 a 1.7.6.14, 1.7.6.20 a 1.7.6.23. Deverá ser apresentado conforme modelo do ANEXO IV – "MODELO DE COMPROVAÇÃO PONTUAL DE ATENDIMENTO À ESPECIFICAÇÃO TÉCNICA

f) prazo de **validade da proposta** que não poderá ser inferior a **60 (sessenta)** dias corridos, contados da data prevista para abertura da licitação.

g) **declaração da licitante de que atenderá integralmente para a execução do contrato as especificações, condições e prazos** estabelecidos neste Edital e seus Anexos.

10.1.2.1. Todos os componentes necessários ao perfeito funcionamento de cada um dos SUBITENS do objeto devem estar discriminados na proposta.

10.1.2.2. Os Manuais técnicos, os atestados de capacidade técnica, bem como os documentos citados na comprovação ponto-a-ponto devem ser preferencialmente em português, mas poderão ser aceitos, excepcionalmente, em língua inglesa, caso não haja a documentação escrita em língua portuguesa.

10.1.2.3. Qualquer item adicional à Planilha de Formação de Preço, que vier a ser necessário para garantir o perfeito funcionamento, quando ocorrer a implantação em campo, será de total responsabilidade da CONTRATADA, não cabendo ônus algum a PGDF.

10.1.2.4. A PGDF poderá fazer diligências/consultas no sentido de sanar dúvidas quanto ao atendimento das especificações relativas aos equipamentos ofertados.

10.1.2.5. A aprovação da Comprovação Pontual de Atendimento às especificações técnicas, suportado pela Equipe Técnica, é condição necessária para a aceitação da proposta do vencedor da licitação.

10.1.2.6.Caso os prazos definidos neste edital não estejam expressamente indicados na proposta e não constar o registro de prazos divergentes dos estabelecidos, eles serão considerados como aceitos pela licitante, ficando esta obrigada ao cumprimento dos mesmos.

10.2. A licitante que abandonar o certame, deixando de enviar a proposta e documentação solicitadas, terá sua proposta desclassificada e sujeitar-se-á às sanções previstas neste edital.

10.3. **O Pregoeiro examinará a proposta** mais bem classificada **quanto à compatibilidade** do preço ofertado **com o valor estimado**, à **conformidade com as especificações técnicas** do objeto licitado e **com os requisitos** estabelecidos neste Edital e seus Anexos, devendo ser desclassificada de forma motivada a que estiver em desacordo.

10.4. Para o julgamento e classificação das propostas, será adotado **o critério de MENOR VALOR GLOBAL DO ITEM,** obtido por meio **da soma do valor total de todos os seus subitens,** observados os prazos máximos para fornecimento, as especificações técnicas e parâmetros mínimos de desempenho e qualidade e demais condições estabelecidas neste Edital.

10.5.O Pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do PGDF ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão.

10.6.Não se considerará qualquer oferta de vantagem não prevista neste edital, inclusive financiamentos subsidiados ou a fundo perdido.

10.7.Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração.

10.8.Será desclassificada a proposta que contenha preço manifestamente inexequível, unitário e total, assim considerado aquele que seja inferior ao custo de produção, acrescido dos encargos legais, desde que a licitante, depois de convocada, não tenha demonstrado a exequibilidade do preço ofertado.

10.9. **Será desclassificada a proposta** que contenha preço excessivo, assim considerado aquele **que for superior ao valor estimado** pela Administração**, unitário e total para os subitens e global** para o item, constante deste Edital/Anexos, observados os princípios da razoabilidade e da proporcionalidade.

XI – DA AMOSTRA/PROVA DE CONCEITO

11.1. De acordo com o item 10 do Termo de Referência, a PGDF solicitará amostra do produto ofertado para realização de prova de conceito com o intuito de sanar dúvidas e comprovar as funcionalidades e requisitos técnicos da solução.

11.2. Após a análise documental da proposta provisoriamente classificada em primeiro lugar, para o item, e verificado o atendimento aos requisitos do Edital, a licitante será convocada, no chat de mensagens do Comprasnet, para a realização da Prova de Conceito, nos termos e prazos estabelecidos no item 10 do Termo de Referência.

11.3. A realização da prova de conceito faz parte dos requisitos de aceitação da proposta.

11.4. Será desclassificada a proposta da licitante que não realizar os testes no prazo concedido e/ou que não tiver a Prova de conceito aprovada.

11.5. Será facultado às demais licitantes ou qualquer interessado, o acompanhamento dos testes da Prova de Conceito, desde que se registrem previamente junto a esta Procuradoria, com antecedência de até 1 (um) dia útil do início dos testes, na condição de ouvinte, ou seja, não será permitido qualquer tipo de interferência nos testes. O acompanhamento ficará limitado a 1 (um) representante por licitante ou interessado, o qual deverá arcar com os respectivos custos de transporte e hospedagem, nos termos do item 10.8 do Anexo I deste Edital.

XII - DA HABILITAÇÃO

12.1. DOCUMENTAÇÃO NECESSÁRIA PARA HABILITAÇÃO:

12.1.1. Habilitação Jurídica

a) Registro comercial, arquivado na Junta Comercial respectiva, no caso de empresa individual.

b) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores.

c) Inscrição do ato constitutivo, no caso de sociedade civis, acompanhada de prova de diretoria em exercício.

d) Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

12.1.2. Regularidade Fiscal e trabalhista

a) Prova de inscrição no Cadastro Nacional da Pessoa Jurídica – **CNPJ**.

b) Prova de **regularidade para com as Fazendas** Estadual e Municipal ou Distrital, do domicílio ou sede da licitante.

c) Prova de **regularidade com a Fazenda Federal** por meio da Certidão Conjunta de Débitos relativos aos Tributos Federais e a Divida Ativa da União, expedida pelo Ministério da Fazenda/Secretaria da Receita Federal do Brasil.

d) para **as empresas com sede ou domicílio fora do Distrito Federal**, certidão Negativa de Débitos ou certidão positiva com efeito de negativa, emitida pela Secretaria de Estado de Fazenda do Governo do Distrito Federal, em plena validade, que poderá ser obtida através do site www.fazenda.df.gov.br. (Inteligência do art. 173, da LODF)

e) Certidão de regularidade de débitos Relativos às **Contribuições Previdenciárias** e às de Terceiros, expedida pela Secretaria da Receita Federal do Brasil.

f) Certificado de Regularidade perante o **FGTS,** fornecido pela Caixa Econômica Federal.

g Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de **Certidão Negativa de Débitos Trabalhistas – CNDT**. (Lei nº 12.440, de 7 de julho de 2011)

12.1.3. Qualificação Técnica:

a) Comprovação de aptidão para desempenho de atividade pertinente e compatível com o objeto desta licitação, mediante **Atestado de Capacidade Técnica**, expedido por pessoa jurídica de direito público ou privado, que comprove que a licitante forneceu e implantou solução de proteção de segurança de informação composta por pelos menos 2 (dois) firewalls *appliance*, operando em cluster ativo/ativo, em uma rede local com no mínimo 400 (quatrocentos) usuários;

b) **Declaração** da Licitante de que realizou **Vistoria Técnica e se** cientificou das peculiaridades, dos atuais equipamentos de rede **e segurança**, das condições no local, do ambiente, das possíveis dificuldades, do padrão das instalações, **configurações e da forma das substituições dos equipamentos de rede da** PGDF, para fins de elaboração da proposta e o devido cumprimento contratual, conforme item 3.4 do Termo de Referência deste edital

(modelo Anexo V-A). Locais definidos no item 5.6 do Termo de Referência. Agendamento pelo telefone: (61) 3325-9661/3325-9667; **ou**

b.1) **Desistência** formal da **Vistoria técnica**, apresentando declaração abdicando do direito de se cientificar das peculiaridades, dos atuais equipamentos de rede **e segurança**, das condições no local, do ambiente, das possíveis dificuldades, do padrão das instalações, **configurações e da forma das substituições dos equipamentos de rede da** PGDF, assumindo total responsabilidade pelo cumprimento das substituições, instalações e configurações dos aparelhos adquiridos e garantia do perfeito funcionamento dos *Firewall*s na rede da PGDF, pelo valor global da proposta.(modelo Anexo V-B)

12.1.4. <u>Qualificação Econômico-Financeira</u>

a) **Certidão Negativa de falência, de concordata, de recuperação judicial ou extrajudicial** (Lei nº 11.101, de 9.2.2005), expedida pelo distribuidor da sede da empresa, datado dos últimos 30 (trinta) dias, ou que esteja dentro do prazo de validade expresso na própria Certidão. No caso de praças com mais de um cartório distribuidor, deverão ser apresentadas as certidões de cada um dos distribuidores.

b) Balanço Patrimonial e demais demonstrações contábeis do último exercício social, já exigíveis e apresentadas na forma da Lei devidamente registrados, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios.

b.1) as empresas constituídas no ano em curso poderão substituir o balanço anual por balanço de abertura, devidamente autenticado pela Junta Comercial;

b.2) a boa situação financeira da empresa será avaliada pelos Índices de Liquidez Geral (LG) e Liquidez Corrente (LC) e Solvência Geral (SG), **superiores a 1 (um)**, resultantes da aplicação das seguintes fórmulas:

$$LG = \frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}}$$

$$LC = \frac{\text{ATIVO CIRCULANTE}}{\text{PASSIVO CIRCULANTE}}$$

$$SG = \frac{\text{ATIVO TOTAL}}{\text{PASSIVO CIRCULANTE+ EXIGÍVEL A LONGO PRAZO}}$$

b.3) As licitantes que apresentarem resultado menor ou igual a 1 (um), em qualquer um dos índices acima, deverão comprovar capital social ou patrimônio líquido de 10% (dez por cento) do **valor global estimado**, constante do Anexo II.

12.1.5. <u>Outros Documentos</u>:

Declaração subscrita por representante legal da licitante, atestando que:

a) Não utiliza mão-de-obra direta ou indireta de menores de 18 (dezoito) anos para a realização de trabalhos noturnos, perigosos ou insalubres, bem como não utiliza, para qualquer trabalho, mão-de-obra direta ou indireta de menores de 16 (dezesseis) anos, exceto na condição de aprendiz, a partir de 14 (quatorze) anos (conforme inciso V do art. 27 da Lei n.º 8.666/93);

b) Havendo superveniência de fato impeditivo à participação no certame, fica a licitante obrigada a declará-lo, sob pena das sanções legais cabíveis.

12.2. <u>DO JULGAMENTO DA HABILITAÇÃO</u>

12.2.1. A licitante habilitada parcialmente no Sistema de Cadastramento Unificado de Fornecedores – SICAF **poderá deixar de apresentar** os documentos relacionados referentes à:

- **habilitação jurídica** (item 11.1.1),
- **regularidade fiscal** (item 11.1.2 com **exceção** das alíneas "d" e "g") e
- **qualificação econômico-financeira** (item 11.1.4 no que se refere a alínea "b" somente se possuir índices de LG e LC e SG superiores a 1 um, caso contrário deverá comprovar capital social ou patrimônio líquido de 10% (dez por cento) do **valor global estimado** constante do Anexo II)

12.2.2. A **comprovação da habilitação parcial no SICAF** dar-se-á mediante a verificação da validade dos documentos necessários, através de consulta on line ao sistema, opção "Situação do Fornecedor" e outras opções de consultas disponíveis, quando do julgamento da habilitação, ocasião que será impressa a respectiva Declaração de "Situação do Fornecedor", sendo a mesma rubricada pelo Pregoeiro.

12.2.3. É assegurado à licitante que esteja com algum documento vencido no SICAF o direito de encaminhar a documentação em plena validade, juntamente com a documentação não contemplada no SICAF prevista neste Edital.

12.2.4. **Os documentos exigidos para a habilitação que não estiverem contemplados** no SICAF ou das licitantes que não optarem pelo cadastramento do SICAF ou com cadastro desatualizado, **deverão ser enviados** no prazo de 03 (três) horas contados a partir da solicitação Pregoeiro no Sistema Eletrônico, preferencialmente **em conjunto com a proposta de preços** em arquivo único, por meio da opção "Enviar Anexo" do Sistema Comprasnet.

12.2.4.1.Os originais ou cópias autenticadas deverão ser enviados, em envelope fechado e identificado o nº do pregão, **no prazo de 03 (três) dias úteis contados a partir da declaração dos vencedores no sistema**, ao protocolo da Procuradoria-Geral do Distrito Federal – PGDF, localizada no Setor de Administração Municipal – SAM- Bloco I, térreo, Brasília/DF, CEP: 70620-000, Telefone: (61) 3342-1086.

12.2.5. Considerando o disposto no art. 97, caput e parágrafo único, da Lei nº 8.666/1993, a recomendação da STC/DF, mediante Circular nº 2/2013-STC e o Acórdão nº 1.793/2011-TCU, será realizado pelo Pregoeiro consulta quanto à existência de registro impeditivo ao direito de participar em licitações ou celebrar contratos com a Administração Pública no módulo SICAF do sistema SIASG e nos endereços eletrônicos a seguir relacionados, sem prejuízo da verificação por outros meios:

12.2.5.1. **no Portal da Transparência do Distrito Federal (http://www.stc.df.gov.br);**

12.2.5.2. **no Cadastro Nacional de Empresas Inidôneas e Suspensas-CEIS/CGU, disponível no Portal da Transparência (http://www.portaltransparencia.gov.br).**

12.2.6.O Pregoeiro poderá consultar sítios oficiais de órgãos e entidades emissores de certidões se necessário, para verificar as condições de habilitação das licitantes, no entanto, não se responsabilizará pela possível indisponibilidade desses sistemas, quando da consulta no julgamento da habilitação, sendo de inteira responsabilidade da licitante a comprovação de sua habilitação. A verificação em sítios oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova.

12.2.7 Para a microempresa ou empresa de pequeno porte, que apresentar a comprovação de regularidade fiscal com alguma restrição, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado vencedor do certame, prorrogáveis por igual período, a critério da Administração, para a regularização da documentação.

12.2.8.A não-regularização da documentação, no prazo previsto no subitem anterior, implicará decadência do direito à contratação, sem prejuízo das sanções previstas neste Edital, e facultará ao Pregoeiro convocar as licitantes remanescentes, na ordem de classificação.

12.2.9.Os documentos necessários para a habilitação poderão ser apresentados em original ou cópia autenticada por cartório competente, ou cópia acompanhada do original para conferência pelo Pregoeiro ou por membro da equipe de apoio ou publicação em órgão da imprensa oficial, ou pela Internet, nos casos em que o órgão responsável pela emissão do documento disponibilizar sua consulta.

12.2.10.Não serão aceitos protocolos de entrega ou solicitação de documentos, em substituição aos documentos requeridos neste Edital e seus Anexos.

12.2.11.Os documentos encaminhados deverão estar em nome da licitante, com indicação do número de inscrição no CNPJ.

12.2.12. Todos os documentos deverão estar em nome e CNPJ da matriz ou todos em nome e CNPJ da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz e os atestados de capacidade técnica, que podem ser apresentados tanto em nome da matriz e/ou em nome da filial.

12.2.13. As certidões que não apresentarem em seu teor, data de validade previamente estabelecida pelo Órgão expedidor, deverão ter sido expedidas até 90 (noventa) antes da data da sessão pública deste Pregão, exceto os documentos que se destinam a comprovação da qualificação econômico-financeira e qualificação técnica.

12.2.14. O pregoeiro, na fase de julgamento, poderá promover quaisquer diligências julgadas necessárias à análise das propostas e da documentação, devendo as licitantes atenderem às solicitações no prazo por ele estipulado, contado do recebimento da convocação.

12.2.15. A não apresentação dos documentos exigidos neste edital implicará inabilitação da licitante, salvo se houver a possibilidade de consulta via internet durante o julgamento da habilitação pelo Pregoeiro.

12.2.16. Verificando-se, no curso da análise, o descumprimento dos requisitos de habilitação estabelecidos neste Edital e seus Anexos, a licitante será inabilitada.

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

12.2.18. Constatado o atendimento pleno às exigências fixadas neste edital, a licitante será declarada vencedora.

XIII – DO RECURSO

13.1 Declarada a vencedora, qualquer licitante poderá, durante a sessão pública, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recurso no prazo de 30 minutos.

13.1.1. A licitante que manifestar a intenção de recurso deverá registrar as razões do recurso, em campo próprio do sistema, no prazo de 3 (três) dias úteis, ficando as demais licitantes, desde logo, intimadas para, querendo, a apresentar contrarrazões, também via sistema, em igual prazo, que começará a contar do término do prazo da recorrente.

13.1.2. A falta de manifestação imediata e motivada da licitante importará na decadência desse direito, ficando o pregoeiro autorizado a adjudicar o objeto à licitante declarada vencedora.

13.1.3. O recurso não acolhido pelo Pregoeiro será apreciado e decidido pela autoridade superior.

13.1.4.O acolhimento de recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

13.1.5.Os autos do processo permanecerão com vistas franqueadas aos interessados na PGDF/DAG, situada no Setor de Administração Municipal – SAM – Projeção “I”, Brasília – DF 2º andar, 204, no horário de 09h as 12h e das 14h as 18h.

13.1.6. Dos atos da Administração cabem:

13.1.6.1. Representação, no prazo de 5 (cinco) dias úteis da intimação da decisão relacionada com o objeto da licitação ou do contrato, de que não caiba recurso hierárquico;

13.1.6.2. Pedido de reconsideração, de decisão do Procurador-Geral do Distrito Federal, conforme o caso, na hipótese do art. 87 da Lei nº 8.666/93, no prazo de 10 (dez) dias úteis da intimação do ato.

XIV– DA ADJUDICAÇÃO E HOMOLOGAÇÃO

14.1. O objeto deste Pregão será adjudicado pelo Pregoeiro, salvo quando houver recurso, hipótese em que a adjudicação caberá à autoridade competente para homologação.

14.2. A homologação deste Pregão compete ao Diretor de Administração-Geral da Procuradoria-Geral do Distrito Federal.

14.3. O objeto deste Pregão será **adjudicado PELO VALOR GLOBAL do item** à licitante vencedora.

XV – DO INSTRUMENTO CONTRATUAL

15.1. Depois de homologada a licitação, será convocada a licitante vencedora para assinatura do contrato no prazo de 5 (cinco) dias úteis a contar da intimação do adjudicatário, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste edital.

15.2.O prazo para a assinatura do contrato poderá ser prorrogado uma única vez, por igual período, quando solicitado pela licitante vencedora durante o seu transcurso, desde que ocorra motivo justificado e aceito pela Chefe da UAG/PGDF, de acordo com o § 1º do art. 64 da Lei nº 8.666/93.

15.3.Para o fiel cumprimento das obrigações contratuais, será exigida da licitante vencedora a prestação de garantia no ato da assinatura do instrumento contratual no valor correspondente a 5% (cinco por cento) do montante do contrato, mediante uma das seguintes modalidades:

I - caução em dinheiro ou em títulos da dívida pública, devendo estes ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda; (Redação dada pela Lei nº 11.079, de 2004)

II - seguro-garantia; (Redação dada pela Lei nº 8.883, de 1994)

III - fiança bancária. (Redação dada pela Lei nº 8.883, de 8.6.94)

15.3.1. O adjudicatário convocado deve apresentar, no prazo máximo de 10 (dez) dias úteis, contado da data da entrega da via do contrato assinada, comprovante de prestação de garantia no valor e nas condições descritas neste Edital.

15.3.2. A garantia somente poderá ser levantada após o cumprimento integral de todas as obrigações contratuais assumidas e a extinção do Contrato;

15.3.3. A garantia ficará retida no caso de rescisão contratual por responsabilidade da Contratada, até a definitiva solução das pendências administrativas ou judiciais que porventura existam.

15.3.4. Sem prejuízo das sanções previstas na lei e neste Edital, a não prestação da garantia exigida será considerada inexecução do Contrato, implicando na imediata anulação da Nota de Empenho emitida e ensejará a rescisão Contratual, nos termos do inciso I do art. 78 da Lei nº 8.666/93.

15.4.Por ocasião da assinatura do contrato e emissão da Nota de Empenho, será exigida a comprovação das condições de habilitação consignadas no edital, as quais deverão ser mantidas pela licitante durante a vigência do contrato.

15.5. Quando a vencedora da licitação não fizer a comprovação referida no subitem acima ou injustificadamente, recusar-se a assinar o contrato, poderá ser convocada outra licitante, desde que respeitada a ordem de classificação, para, após comprovados os requisitos habilitatórios e feita a negociação, assinar o contrato, sem prejuízo das multas previstas neste edital e no contrato e das demais cominações legais

15.6. Farão parte integrante do contrato este Edital e seus Anexos e a proposta Apresentada pela licitante vencedora.

15.7. O contrato poderá ser alterado na ocorrência de quaisquer fatos estipulados no Art. 65 da Lei n.º 8.666/93 e suas alterações.

15.8 O contrato poderá ser rescindido, conforme as disposições dos artigos 77 a 80 da Lei nº 8.666/93.

15.9. Incumbirá à contratante providenciar a publicação resumida do instrumento do contrato e de seus eventuais termos aditivos, no Diário Oficial do Distrito Federal.

15.10. É vedada a subcontratação, cessão ou transferência parcial ou total do objeto deste edital.

XVI – DA VIGÊNCIA DO INSTRUMENTO CONTRATUAL

16.1.O prazo de **vigência do contrato será de 51 (cinquenta e um) meses**, a contar da data de sua assinatura, com eficácia a partir de sua publicação, compreendendo os prazos de entrega dos equipamentos, de procedimentos de recebimento fixados, da instalação e configuração da solução, passagem de conhecimento, bem como da garantia, onde neste caso, iniciar-se-á a contagem a partir do recebimento definitivo da solução.

XVII – DAS OBRIGAÇÕES DA CONTRATADA

17.1. Zelar pela perfeita execução dos serviços contratados, prestando-os sem interrupção;

17.2. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no ato convocatório;

17.3. Responder pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato.

17.4. Responsabilizar-se por quaisquer danos pessoais e/ ou materiais, causados por seus empregados diretamente à Administração ou a terceiros, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pela contratante;

17.5. Responsabilizar-se pelas eventuais despesas para execução do serviço solicitado, qualquer que seja o valor.

17.6. Não transferir a qualquer título os serviços contratados;

17.7.Independentemente de transcrição na proposta, sujeitar-se às demais obrigações estabelecidas no Termo de Referência (Anexo I e I.1) deste Edital.

17.8. Cumprir todas as especificações, obrigações e cláusulas estabelecidas neste Edital e seus Anexos.

17.9. Comunicar à contratante, por escrito, qualquer anormalidade de caráter urgente e prestar, com a devida antecedência, os esclarecimentos necessários;

17.10. Assumir inteira responsabilidade técnica e administrativa sobre o objeto contratado, não podendo transferir a outras empresas a responsabilidade pelos serviços;

17.11. Providenciar a imediata correção das deficiências, falhas ou irregularidades apontadas pela Contratante na execução do serviço, atendendo às solicitações do executor do contrato, voltadas ao saneamento e correção da(s) irregularidade(s) verificada(s);

17.12. Não fazer uso de mão de obra infantil, nos termos da **Lei Distrital nº 5.061/2013.**

17.13. Adotar na execução dos serviços, práticas de sustentabilidade ambiental, a recepção de bens, embalagens, recipientes ou equipamentos inservíveis e não reaproveitáveis pela PGDF, práticas de desfazimento sustentável, reciclagem dos bens inservíveis e processos de reutilização, nos termos estabelecidos na Lei Distrital nº 4.770, de 22 de fevereiro de 2012, que sejam aplicáveis ao objeto deste contrato.

XVIII – DAS OBRIGAÇÕES DA CONTRATANTE

18.1. Indicar o executor interno do Contrato, conforme art. 67 da Lei 8.666/93.

18.2. Cumprir os compromissos financeiros assumidos com a Contratada;

18.3. Fornecer e colocar à disposição da Contratada todos os elementos e informações que se fizerem necessários à execução dos serviços;

18.4. Notificar, formal e tempestivamente, a contratada sobre as irregularidades observadas no serviço;

18.5. Notificar a Contratada, por escrito e com antecedência sobre multas, penalidades quaisquer débitos de sua responsabilidade.

XIX - DA FISCALIZAÇÃO

19.1. A execução dos serviços será acompanhada e fiscalizada por executor interno do ajuste, especialmente designado, que anotará em registro próprio todas as ocorrências, determinando o que for necessário à regularização das faltas ou defeitos observados, além das atribuições contidas nas Normas de Execução Orçamentária e Financeira do Distrito Federal;

19.2. Não obstante a Contratada seja única e exclusiva responsável pela execução de todos os serviços definidos neste edital e seus Anexos, a Contratante reserva-se o direito de exercer a mais ampla fiscalização sobre os serviços, por intermédio de representante especificamente designado, sem que de qualquer forma restrinja essa responsabilidade, podendo:

19.2.1. Exigir a substituição de qualquer empregado ou preposto da contratada que, a seu critério, venha a prejudicar o bom andamento dos serviços;

19.2.2. Determinar a correção dos serviços realizados com falha, erro ou negligência, lavrando termo de ocorrência do evento;

XX – DO RECEBIMENTO

20.1 O objeto desta licitação será recebido por servidor ou comissão designada pela autoridade competente, mediante termo circunstanciado, assinado pelas partes, da seguinte forma:

a) provisoriamente, para efeito de posterior verificação da conformidade do objeto com a especificação, nos termos e prazo definido no **item 6.6** do Termo de Referência deste edital; e

b) definitivamente, após o decurso do prazo de observação ou vistoria que comprove a adequação do objeto aos termos contratuais, nos termos e prazo definido no **item 6.6** do Termo de Referência deste edital**.**

20.2. Após o recebimento definitivo do objeto, será atestada a Nota Fiscal/Fatura, para efeito de pagamento;

20.3. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do serviço, nem ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo contrato;

20.4. Se a licitante vencedora deixar de disponibilizar o serviço dentro do prazo estabelecido sem justificativa por escrito e aceita pela Administração, sujeitar-se-á às penalidades impostas neste Edital;

XXI – DO PAGAMENTO

21.1. Para efeito de pagamento, a PGDF consultará os sítios oficiais dos órgãos e entidades emissores das certidões a seguir relacionadas, **para a verificação da regularidade fiscal da Contratada:**

a) **Certidão de regularidade** de débitos Relativos às **Contribuições Previdenciárias** e às de Terceiros, expedida pela Secretaria da Receita Federal do Brasil (Decreto Federal nº 6.106/2007);

b) Certificado de **Regularidade do Fundo de Garantia por Tempo de Serviço** – FGTS, fornecido pela CEF – Caixa Econômica Federal, devidamente atualizado (Lei n.º 8.036/90);

c) Certidão de **Regularidade** com **a Fazenda do Distrito Federal.**

d) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de **Certidão Negativa de Débitos Trabalhistas** – **CNDT** (Lei nº 12.440, de 7 de julho de 2011).

21.1.2. Em havendo a impossibilidade de consulta, pela Administração, aos sítios oficiais dos órgãos e entidades emissores das citadas certidões, o pagamento ficará condicionado à apresentação, pela **Contratada, da comprovação de sua regularidade fiscal e trabalhista.**

21.1.3. A Contratada deverá observar o disposto na Lei nº 5.087 de 25.03.2013 do Distrito Federal.

21.2. O pagamento da solução de segurança da informação (*firewalls appliance*s, sistema de gerencia e monitoração, serviços de instalação e configuração, passagem de conhecimento) **será integral,** de acordo com o estabelecido no **item 6.7.1** do Termo de Referência, anexo I deste Edital**,** realizado em até 30 (trinta) dias, contados a partir da data de apresentação da Nota Fiscal/Fatura, atestada pelo Executor do Contrato, desde que o documento de cobrança esteja em condições de liquidação e pagamento.

21.2.1. O pagamento do serviço de suporte técnico será efetuado **mensalmente**, em até 30 (trinta) dias, somente após o recebimento definitivo da solução, mediante atesto do gestor do contrato, comprovando o perfeito funcionamento da solução e prestação do serviço de suporte técnico, além da Nota Fiscal/Fatura referente a estes serviços prestados, bem como do relatório detalhado de serviço, conforme item 6.7.2 do Termo de Referência.

21.3. Passados 30 (trinta) dias sem o devido pagamento por parte da Administração, a parcela devida será atualizada monetariamente, desde o vencimento da obrigação até a data do efetivo pagamento de acordo variação do **Índice Nacional de Preços ao Consumidor Amplo– IPCA**.

21.4. Nenhum pagamento será efetuado à licitante enquanto pendente de liquidação qualquer obrigação que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária (quando for o caso).

21.5. As empresas com sede ou domicílio no Distrito Federal, com créditos de valores iguais ou superiores a R$ 5.000,00 (cinco mil reais), terão seus pagamentos feitos exclusivamente mediante crédito em conta corrente, em nome do beneficiário junto ao Banco de Brasília S/A – BRB. Para tanto deverão apresentar o número da conta corrente e da agência em que desejam receber seus créditos, de acordo com o Decreto n.º 32.767 de 17/02/2011, publicado no DODF nº 35, pág. 3, de 18/02/2011.

21.6. Será efetuada a retenção na fonte dos tributos e contribuições prevista na Instrução Normativa SRF nº 480/2004, alterada pela IN nº 539/2005.

21.7. A retenção dos tributos não será efetivada caso a licitante apresente junto com sua Nota Fiscal/Fatura a comprovação de que ele é optante do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte –SIMPLES.

21.8. O pagamento dar-se-á mediante emissão de Ordem Bancária – OB, junto ao Banco de Brasília S.A., em Brasília-DF, ou tratando-se de empresa de outro Estado que não tenha filial ou representação no Distrito Federal, junto ao banco indicado, conforme Decreto nº 18.126/97, no prazo de 30 (trinta) dias corridos contados da data de apresentação pela Contratada da documentação fiscal correspondente e após o atestado da fiscalização da PGDF.

21.9. Documentos de cobrança rejeitados por erros ou incorreções em seu preenchimento serão formalmente devolvidos à Contratada, no prazo máximo de 5 (cinco) dias úteis contados da data de sua apresentação.

21.10. Os documentos de cobrança, escoimados das causas que motivaram a rejeição, deverão ser reapresentados num prazo máximo de 02 (dois) dias úteis.

21.11. Em caso de rejeição da Nota Fiscal/Fatura, motivada por erro ou incorreções, o prazo de pagamento passará a ser contado a partir da data de sua reapresentação.

XXII – DAS SANÇÕES

22.1. As licitantes e/ou contratadas que não cumprirem integralmente as obrigações assumidas, garantida a prévia defesa, ficam sujeitas às sanções estabelecidas no Decreto nº 26.851, de 30/05/2006, publicado no DODF nº 103, de 31/05/2006, pg. 05/07, com suas **alterações**. Cópia integrante do **Anexo XI.**

XXIII– DA CLASSIFICAÇÃO ORÇAMENTÁRIA

23.1. Unidade Orçamentária: 120901 – Fundo da Procuradoria-Geral do Distrito Federal

23.2. Programa de Trabalho: 03.126.6003.1471.0034 e 03.126.6003.2557.0019

23.3. Natureza da Despesa: 44.90.52 e 33.90.39

XXIV – DA DISPOSIÇÕES FINAIS

24.1. A PGDF poderá revogar este Pregão por razões de interesse público decorrente de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-lo por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado.

24.1.1. A anulação do pregão induz à do contrato.

24.1.2. As licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito da contratada de boa-fé de ser ressarcida pelos encargos que tiver suportado no cumprimento do contrato.

24.2.É facultado ao Pregoeiro ou à autoridade superior, em qualquer fase desde Pregão, promover diligência destinada a esclarecer ou completar a instrução do processo, vedada a inclusão posterior de informação ou de documentos que deveriam ter sido apresentados para fins de classificação e habilitação.

24.3. No julgamento das propostas e na fase de habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas e dos documentos e a sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de classificação e habilitação. (§3º do art. 26 do Dec. nº 5.450/2005)

24.4. O Pregoeiro prorrogará por igual período, o prazo estabelecido de 03 (três) horas, contados a partir da solicitação no Sistema Eletrônico, para envio da proposta e documentação, por meio da opção “Enviar Anexo” do Sistema Comprasnet, quando solicitado e justificado pela licitante e antes do término do prazo concedido.

24.5. Na contagem dos prazos estabelecidos neste edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na PGDF.

24.6. O desatendimento às exigências formais, não essenciais, não importará na inabilitação da licitante e/ou desclassificação de sua proposta, desde que seja possível a aferição de sua habilitação e a exata compreensão da sua proposta, durante a realização da sessão pública do pregão.

24.7. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da administração, o princípio da isonomia, a finalidade e a segurança da contratação. (Parágrafo único do art. 5º do Dec. nº 5.450/2005)

24.8. A autoridade competente poderá, em qualquer fase do processo licitatório, desclassificar a proposta da licitante que for declarada inidônea na área da Administração Pública, assegurada a ampla defesa.

24.9.

E

ste Pregão poderá ter a data de abertura da sessão pública transferida por conveniência do PGDF.

24.10. O foro para dirimir questões relativas ao presente edital será o de Brasília – DF, com exclusão de qualquer outro.

24.11. Os casos omissos e demais dúvidas suscitadas serão dirimidas pelo Pregoeiro, por meio do Telefone: (61) 3342-1086.

24.12. **Havendo irregularidades neste instrumento**, entre em contato com a Ouvidoria de Combate à Corrupção, no telefone 0800-6449060. (**Decreto nº 34.031/2012,** publicado no DODF de 13/12/2012 p 5.)

XXV– DOS ANEXOS

25.1. Fazem parte integrante deste Edital os seguintes Anexos:

25.1.1. ANEXO I -Termo de Referência;

25.1.2. ANEXO I.1 - Características Técnicas Mínimas Obrigatórias

25.1.3. ANEXO II - Planilha Estimativa de Custos

25.1.4. ANEXO III - Modelo de Proposta

25.1.5. ANEXO IV - Modelo de comprovação pontual de atendimento à especificação técnica

25.1.6. ANEXO V-A - Modelo de Declaração de Vistoria Técnica

25.1.7. ANEXO V-B - Modelo de Declaração de Desistência de Vistoria técnica,

25.1.8. ANEXO VI - Modelo de Declaração de que Não Emprega Menor

25.1.9. ANEXO VII - Modelo de Termo de Confidencialidade

25.1.10.ANEXO VIII - Modelo de Termo de Recebimento Provisório

25.1.11.ANEXO IX - Modelo de Termo de Recebimento Definitivo

25.1.12.ANEXO X - Minuta do Contrato.

25.1.13. ANEXO XI - Cópia do Decreto nº 26.851/2006 - Regula a aplicação de penalidades do DF.

Brasília, 15 de setembro 2015

BÁRBARA HAMÚ
Pregoeira

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de empresa para fornecimento de solução de segurança de rede, composta por 6 (seis) *firewalls appliances*, sistema de gerencia e monitoração centralizada, serviços de instalação e configuração, transferência de conhecimento, garantia e suporte técnico on-site, conforme especificações técnicas contidas neste Termo de Referência e seus anexos.

1.2. Relação dos Produtos:

ITEM	SUBITEM	BEM / SERVIÇO	QTDE	Un.
1	1.1	Firewall Appliance Tipo 1	2	Solução
	1.2	Firewall Appliance Tipo 2	2	Solução
	1.3	Firewall Appliance Tipo 3	2	Solução
	1.4	Gerência e Monitoração Centralizada	1	Sistema
	1.5	Instalação e Configuração	1	Serviço
	1.6	Transferência de Conhecimento	1	Turma
	1.7	Suporte Técnico	48	Meses

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. FUNDAMENTAÇÃO LEGAL DA AQUISIÇÃO

2.1.1. Este Planejamento da Contratação foi elaborado à luz dos dispositivos legais, a saber:

a. Lei nº 8.666/1993 - Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.

b. Lei nº 10.520/2002 - Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências.

c. Decreto nº 5.450/2005 – Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providencias.

d. Instrução Normativa SLTI nº 4/2010 - Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. Essa norma aplica-se subsidiariamente à IN/SLTI 02/2008.

e. Decreto nº 34.637/2013, que recepcionou no âmbito da Administração Direta e Indireta do Distrito Federal a IN MP/SLTII nº 4/2010.

f. Decreto nº 7.174/2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.

g. Decreto nº 32.218/2010, que recepcionou no âmbito da Administração Direta e Indireta do Distrito Federal o Decreto Federal nº 7.174/2010.

h. Nota Técnica nº 01/2008 - SEFTI/TCU - Estabelece o conteúdo mínimo do projeto básico ou Termo de Referência para contratação de serviços de Tecnologia da Informação e Comunicações – TIC.

i. Nota Técnica nº 02/2008 - SEFTI/TCU - Estabelece o uso do pregão para aquisição de bens e serviços de Tecnologia da Informação.

j. Lei Distrital nº 2.605/2000 – Institui o Fundo da Procuradoria Geral do Distrito Federal – PRÓ-JURÍDICO.

k. Decreto nº 21.936/2001 – Aprova o Regimento Interno do Fundo da Procuradoria Geral do Distrito Federal – Pró Jurídico e dá outras providências.

l. Decreto nº 33.528/2012 – Dispõe sobre a aprovação de Estratégia Geral de Tecnologia da Informação – EGTI, elaborada pelo Comitê Gestor de Tecnologia da Informação e Comunicação e dá outras providências.

2.1.2. Esse instrumento também guarda observância à lei de licitações para contratação de bens na administração pública, Planejamento Estratégico (PEI), iniciativa estratégica: item 8 e 9, Plano Diretor de Tecnologia da Informação (PDTI), necessidade 10.1.b, meta 11.2 e investimento previsto 12.2 e também ao projeto de informatização da Procuradoria Geral do DF intitulada de "Projeto PGDF Digital".

2.2. CARACTERIZAÇÃO DA SOLUÇÃO

2.2.1. O Decreto nº 5.450, de 31/05/2005 estabelece em seu parágrafo primeiro do artigo 2º que se consideram bens e serviços comuns, aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado, dessa forma, o objeto deste instrumento caracteriza-se por **BENS E SERVIÇOS COMUNS** devido aos seus padrões de desempenho e de qualidade serem facilmente definidos por meio de especificações usuais de mercado, onde são ofertados, em princípio, por muitos fornecedores e comparáveis entre si com facilidade, conforme Acórdão nº 2.471/2008-TCU-Plenário.

2.3. MODALIDADE DE LICITAÇÃO

2.3.1. No artigo 4º do mesmo Decreto nº 5.450, de 31/05/2005, estabelece que nas licitações para aquisição de bens e serviços comuns será obrigatória a modalidade pregão, sendo preferencial a utilização da sua forma eletrônica, com isso, define-se a modalidade de licitação como **PREGÃO ELETRÔNICO**.

2.3.2. Podemos citar também o entendimento da Nota Técnica nº 02/2008 (SEFTI/TCU), que estabelece obrigatoriamente o uso do pregão para licitação de bens e serviços de Tecnologia da Informação considerados comuns, conforme transcrição abaixo:

Entendimento I. A licitação de bens e serviços de tecnologia da informação considerados comuns, ou seja, aqueles que possuam padrões de desempenho e de qualidade objetivamente definidos pelo edital, com base em especificações usuais no mercado, deve ser obrigatoriamente realizada pela modalidade Pregão, preferencialmente na forma eletrônica.

2.4. TIPO DE LICITAÇÃO

2.4.1. **MENOR PREÇO**.

2.5. JUSTIFICATIVA DO NÃO PARCELAMENTO DO OBJETO

2.5.1. O objeto não poderá ser parcelado em virtude das seguintes justificativas:

2.5.1.1. Para não impossibilitar tecnicamente a implementação total da solução, caso os itens sendo licitados separadamente, em um eventual insucesso de um ou mais itens, possibilitaria a

contratação de apenas parte dos itens. Dessa forma, a adjudicação do certame para um único vencedor, visa resguardar a efetividade do processo de aquisição.

Evitar problemas de interoperabilidade e assistência técnica da solução de *Firewall Appliance*, em uma situação de manutenção seja ela corretiva ou preventiva, imagine que haja vários vencedores para os itens da licitação, como seria o problema na solicitação de um atendimento, onde num mesmo ambiente físico e lógico de alta complexidade, existem mais de uma entidade fazendo alterações? No caso de uma pane, haveria dificuldade de identificar o equipamento/software ou configuração defeituosa, necessitando assim, a convocação de vários fornecedores, e qual seria o custo/tempo para reestabelecimento da normalidade do ambiente, onde milhares de usuários acessam simultaneamente os diversos serviços disponibilizados? Ainda mais agora, que a Procuradoria está passando por um processo de Informatização dos Auto Suplementares, o qual ficará na forma Digital, há a necessidade da infraestrutura de segurança da informação estar funcionando o tempo todo, e em eventuais falhas, que o serviço volte a funcionar o mais rápido possível para evitar perdas e prazos judiciais.

2.5.1.2. O objeto de contratação é composto por uma solução de segurança da informação que funcionará de forma integrada permitindo a conexão e comunicação dos equipamentos e sistemas internos com a rede externa (internet) de forma segura. A aquisição em um só grupo é praticada em todos os órgãos públicos pesquisados, e justificada pela condição técnica de intercomunicação, compatibilidade e padronização entre os equipamentos e instalações, reduzindo riscos e conflitos.

2.5.2. Dessa forma, o objeto não foi parcelado.

2.6. SITUAÇÃO ATUAL E JUSTIFICATIVA DA CONTRATAÇÃO

2.6.1. A Procuradoria-Geral do Distrito Federal - PGDF, órgão central do sistema jurídico do Distrito Federal, é uma instituição de natureza permanente, essencial à Justiça e à Administração, cabendo-lhe a representação judicial e a consultoria jurídica do Distrito Federal, como atribuições privativas dos Procuradores do Distrito Federal, na forma do art. 132 da Constituição Federal.

2.6.2. A Procuradoria-Geral do Distrito Federal, que é equiparada, para todos os efeitos, às Secretarias de Estado, tem por finalidade exercer a advocacia pública, cabendo-lhe, ainda, prestar a orientação normativa e a supervisão técnica do sistema jurídico do Distrito Federal. Compete, também, ao órgão: representar o Distrito Federal judicial e extrajudicialmente; zelar pelo cumprimento, na Administração Pública Direta e Indireta, das normas jurídicas, das decisões judiciais e dos pareceres jurídicos da PRG/DF; orientar sobre a forma de cumprimento de decisões judiciais e pedidos de extensão de julgados relacionados com a Administração Direta do Distrito Federal; efetuar a cobrança judicial da dívida do Distrito Federal; e promover a uniformização da jurisprudência administrativa e a compilação da legislação do Distrito Federal.

2.6.3. Seguindo esta linha, a Casa vem atuando na implementação de soluções tecnológicas que atendam as condições de trabalho dos Procuradores, bem como a sustentabilidade de sua estrutura administrativa na execução de serviços.

2.6.4. A rede local da PGDF está hoje, por questões de segurança, isolando o tráfego e gerenciando de forma segmentada. Cada um desses segmentos cumpre um papel importante na estrutura geral da TI. Como elemento de interligação dessas sub-redes, a PGDF possui 2 (dois) equipamentos *firewall appliance* operando em modo ativo-passivo, ou seja, apenas um deles está efetuando a análise do tráfego, enquanto o outro permanece em *stand-by* para entrar em operação no caso de alguma falha do outro equipamento. Assim, o firewall e as regras neles existentes determinam quais pacotes irão trafegar entre os diversos segmentos. Por conta

disso, esses equipamentos são de vital importância, não só para o perfeito funcionamento da rede local da PGDF, como também para garantir a sua segurança.

2.6.5. Ocorre que esses equipamentos não suportam mais processar adequadamente todo o tráfego gerado pelos usuários da rede local da PGDF, ocasionando perda de desempenho em todos os acessos. Os atuais equipamentos estão tecnologicamente ultrapassados e não refletem mais segurança no atual cenário de tecnologia mundial.

2.6.6. De modo similar, os atuais equipamentos também não conseguirá processar todo o futuro tráfego da Casa, já que a PGDF está aumentando a capacidade de armazenamento e processamento através do novo Datacenter, do site Backup, e dos diversos novos sistemas que estão entrando (ou que entrarão brevemente) em produção.

2.6.7. Os ataques às redes corporativas e as formas de burlar os bloqueios existentes se tornaram demasiadamente elaborados, eficiente e complexos. Os atuais dispositivos em operação não conseguem mais fazer a análise adequada desses mecanismos complexos. Hoje a PGDF carece de uma ferramenta que possa inibir que certos dados sejam perdidos.

2.6.8. Dessa forma, dada à importância que o firewall possui para a operação e segurança da rede local da PGDF, torna-se necessária a aquisição de novos equipamentos capazes de suprir a atual demanda de processamento, bem como futuras expansões, além de possuírem uma tecnologia mais recente de análise dos pacotes que trafegam entre as redes, possibilitando a identificação e o bloqueio de ataques complexos, provendo a segurança dos dados e da rede local da PGDF.

2.6.9. Ademais, está sendo implantado o principal sistema da Casa que tornará os processos de Autos-Suplementares (AS) em uma forma digital. Dessa forma, é imprescindível que haja segurança de forma efetiva que proteja a informação e a mantenha de forma integra e disponível. Para isso, está sendo implementado o novo datacenter e o site backup, os quais precisarão de mecanismos de segurança para manter os serviços de TI. É exatamente essa aquisição de solução de firewall que proverá toda segurança necessária para que os serviços de TI permaneçam íntegros, confidenciais e disponíveis para a Casa.

2.6.10. Além disso, os relatórios que podem ser gerados pela atual solução são insuficientes para as análises da equipe da Gerencia de Produção e Rede da Casa. A PGDF necessita de relatórios técnicos e gerenciais sobre a segurança dos equipamentos, dos serviços de TI e de detecção de intrusão, vírus e de ataques.

2.7. PAPEL SIMPLIFICADO DO FIREWALL

2.7.1. Para definir o papel do firewall de forma simplificada, podemos usar a seguinte associação: Para que ladrões não entrem em sua casa, você deve trancar suas portas e janelas, ou instalar grades, alarmes e sistemas de segurança, dificultando o acesso ao interior do imóvel. O Firewall tem função similar, pois “tranca” todas as portas e janelas dos ativos de TI (computador, datacenter, etc.) para que só os autorizados possam entrar e sair. O Firewall vai tornar os dados da Procuradoria mais seguros;

2.7.2. Os equipamentos tipo firewall consistem em ativos de rede que têm como função controlar o tráfego entre redes distintas e impedir a transmissão ou recepção de acessos nocivos ou não autorizados de uma rede para outra, protegendo os recursos de hardware e software, em conformidade a um determinado conjunto de regras de segurança.

2.7.3. Por meio da inspeção dos pacotes de rede que passam por seu controle, o firewall possui a habilidade de bloquear tráfego de entrada indesejado (vírus, trojans, pragas, etc. ...), baseado nos endereços de origem e de destino, bloquear tráfego de acordo com o conteúdo ou permitir acesso às redes protegidas a partir da internet, desde que atendidos alguns requisitos de autenticidade. Outra função importante dos firewalls corporativos é a possibilidade de gerar relatórios das atividades e do tráfego de rede para monitoramento da segurança.

2.7.4. O firewall também é uma importante ferramenta contra *malwares*, através da funcionalidade de varrer os pacotes de rede em tempo real com o uso de técnicas de bloqueio de assinatura, reconhecimento de arquivos, heurísticas, checagem de endereço IP, checagem de URL, dentre outras.

2.8. DOS BENEFICIOS E RESULTADOS

2.8.1. Provisão de segurança para o novo Data Center e para o site backup;

2.8.2. Garantia de disponibilidade e continuidade dos serviços oferecidos;

2.8.3. Garantia de integridade das informações fornecidas;

2.8.4. Aumento da velocidade suportado pelas interfaces da solução de Firewall;

2.8.5. Aumento do *throughput* da solução de Firewall;

2.8.6. Agregação de confiabilidade aos serviços prestados;

2.8.7. Agregação de valor aos serviços prestados pela informática da PGDF;

2.8.8. Provisão de gestão da Segurança da Informação de forma mais efetiva;

2.8.9. Melhoria na aplicação das regras e políticas de segurança da informação;

3. DESCRIÇÃO DA SOLUÇÃO DE TI

3.1. DESCRIÇÃO

3.1.1. A solução de TI escolhida é a contratação de empresa para fornecimento de solução de segurança de rede em alta disponibilidade, composta por 6 (seis) *firewalls appliances*, sistema de gerência e monitoração centralizada, serviços de instalação e configuração, transferência de conhecimento, garantia e suporte técnico on-site, conforme especificações.

3.2. RELAÇÃO DE BENS E SERVIÇOS

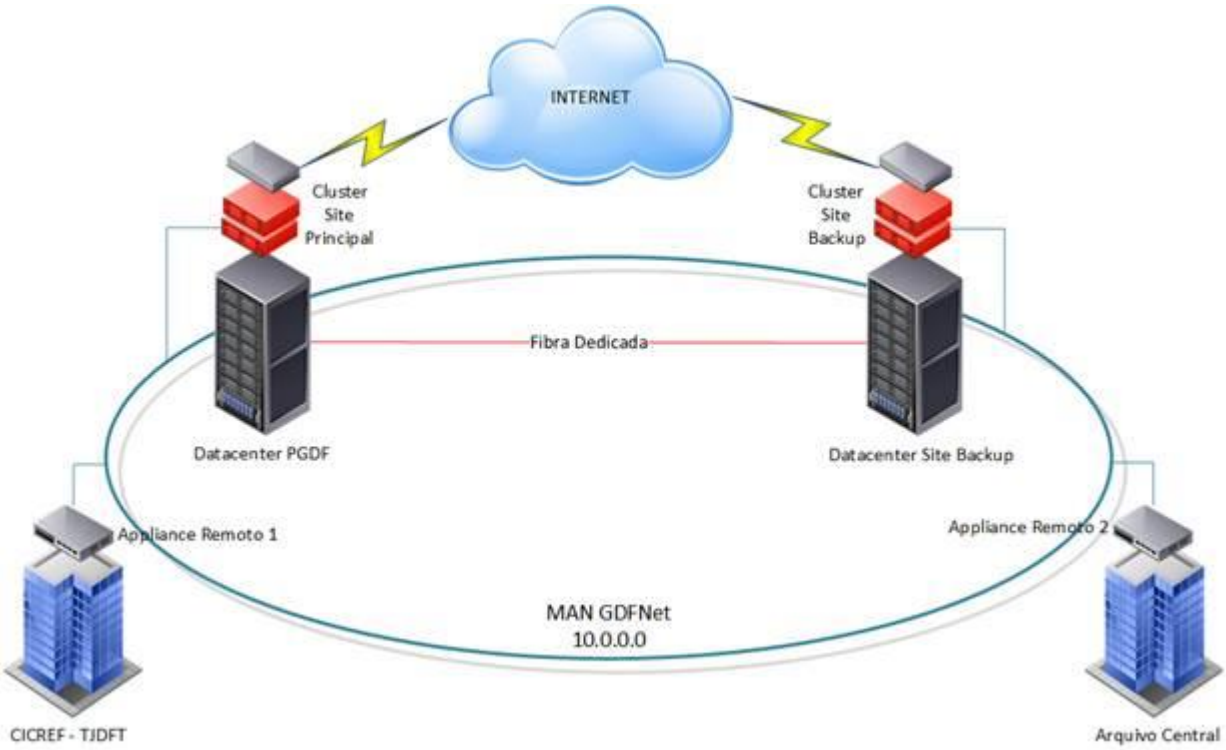
BEM / SERVIÇO	QTDE	Un.
Firewall Appliance Tipo 1	**2**	**Solução**
Firewall Appliance Tipo 2	**2**	**Solução**
Firewall Appliance Tipo 3	**2**	**Solução**
Gerência e Monitoração Centralizada	**1**	**Sistema**
Instalação e Configuração	**1**	**Serviço**
Transferência de Conhecimento	**1**	**Turma**

Suporte Técnico	**48**	**Meses**

3.3. ARQUITETURA

3.3.1. O Firewall Appliance Tipo 1 está representado na figura adentro do ambiente do Datacenter PGDF (Cluster Site Principal), o Firewall Appliance Tipo 2 está representado na figura adentro do ambiente do Datacenter Site Backup (Cluster Site Backup) e o Firewall Appliance Tipo 3, que são departamentos da PGDF localizados em outros endereços, e estão representados na figura abaixo adentro dos ambientes da GECONFI (Prédio do TJ - Appliance Remoto 1) e do Arquivo Central (Appliance Remoto 2).

3.3.2. Nessa solução que consiste em 6 (seis) equipamentos, sendo que 4 (quatro) equipamentos deverão compor 2 (dois) clusters ativo-ativo, sendo um cluster instalado no site principal, localizado no endereço SAM Projeção I e o outro no site backup, no endereço SAM Projeção H. Os outros 2 (dois) equipamentos tem menos poder de processamento e ficarão: a) Arquivo Central; b) GECONFI, escritório localizado dentro do TJ; onde tais unidades se conectarão ao edifício sede da Procuradoria Geral do DF, conforme figura abaixo:



3.4. DA VISTÓRIA

3.4.1. As interessadas deverão realizar vistoria nas instalações desta PGDF onde serão instalados os equipamentos ou no caso da opção pela não realização da vistoria, apresentar declaração abdicando do direito de se cientificar das peculiaridades, dos atuais equipamentos de rede e de segurança, das condições no local, do ambiente, das possíveis dificuldades, do padrão das instalações, configurações e da forma dos equipamentos de rede da procuradoria geral do DF, assumindo total responsabilidade pelo cumprimento das substituições, instalações e configurações dos aparelhos adquiridos e garantia do perfeito funcionamento da Solução de

Firewall Appliance na rede da PGDF, CONFORME ANEXO V-B – MODELO DE DECLARACAO DE DESISTÊNCIA DE VISTORIA TÉCNICA, O QUAL DEVERÁ SER ANEXADO JUNTAMENTE COM A DOCUMENTAÇÃO DE HABILITAÇÃO;

3.4.2. A vistoria técnica tem como objetivo que a licitante se cientifique das peculiaridades, dos atuais equipamentos de rede e de segurança, das condições no local, do ambiente, das possíveis dificuldades, do padrão das instalações, configurações e da forma das substituições dos equipamentos de rede da Procuradoria Geral do DF (PGDF), assumindo total responsabilidade pelo cumprimento das substituições, instalações e configurações dos aparelhos adquiridos e garantia do perfeito funcionamento da Solução de *Firewall Appliance* na rede da PGDF, CONFORME ANEXO V-A – MODELO DE DECLARACAO DE VISTORIA TÉCNICA;

3.4.3. O requisito de vistoria se faz necessário para que os licitantes tenham condições de absorver a maior quantidade de informações necessárias para a elaboração de suas propostas e o devido cumprimento contratual pela vencedora, com o objetivo de garantir maior segurança para a administração pública.

3.4.4. A vistoria técnica deverá ser realizada no prazo de até 1 (um) dia antes da data de abertura da licitação;

3.4.5. O agendamento da vistoria deverá ser previamente efetuado por meio dos telefones (61) 3325-9661 / (61) 3325-9667 (colaborador do setor DISIS/GEPRO), mencionando o número do edital, as informações de contato da licitante que efetuará a vistoria;

3.4.6. Efetuada a vistoria será lavrado, por representante da Procuradoria Geral do DF, designado para tanto, o respectivo atestado de vistoria, conforme ANEXO V-A – MODELO DE DECLARACAO DE VISTORIA TÉCNICA, o qual deverá ser preenchido e assinado por responsável do interessado em participar da licitação, que deverá ser anexado juntamente com a documentação de habilitação;

4. ESPECIFICAÇÕES TÉCNICAS

4.1. CARACTERÍSTICAS TÉCNICAS MÍNIMAS EXIGIDAS

4.1.1. As características técnicas mínimas exigidas estão descritas no ANEXO I.1 – CARACTERÍSTICAS TÉCNICAS MÍNIMAS OBRIGATÓRIAS – deste Termo de Referência.

5. MODELO DE PRETAÇÃO DE SERVIÇO / FORNECIMENTO DE BENS

5.1. DO PROJETO DE IMPLANTAÇÃO DA SOLUÇÃO

5.1.1. A Contratada deverá se reunir com a Contratante nas dependências da PGDF para o levantamento das necessidades do projeto com vistas a subsidiar a elaboração de um Projeto de Implantação da Solução, que deverá conter no mínimo:

5.1.1.1. Cronograma de implantação da solução;

5.1.1.2. Descrição de fases, etapas e atividades que serão executadas na instalação e configuração;

5.1.1.3. Cronograma da passagem de conhecimento, contendo pelo menos o detalhamento do conteúdo programático, a priorização e distribuição do conteúdo e os dias de realização do curso;

5.1.1.4. Recursos envolvidos (humanos e tecnológicos);

5.1.1.5. Diagramas de implantação dos componentes;

5.1.1.6. Explicação resumida da configuração dos equipamentos.

5.1.2. A PGDF poderá solicitar a reformulação do projeto e sugerir inclusões, exclusões e/ou alterações em seu conteúdo.

5.2. PASSAGEM DE CONHECIMENTO

5.2.1. A passagem de conhecimento oferecido deverá ser ministrado por técnico certificado pelo fabricante dos equipamentos;

5.2.2. A passagem de conhecimento para os participantes indicado pela PGDF, incluirá, no mínimo, 40 (quarenta) horas de capacitação;

5.2.3. O treinamento tem como objetivo transferir o conhecimento necessário para administrar e operacionalizar os equipamentos e sistemas integrantes da solução contratada;

5.2.4. O conteúdo do treinamento deverá ser de natureza teórica e prática, devendo abranger todos os equipamentos, componentes e softwares dos módulos a serem instalados, em seus aspectos mais relevantes e, em especial, envolvendo aqueles relacionados à solução implantada no ambiente computacional da PGDF, contendo, no mínimo:

5.2.4.1. Apresentação do projeto a ser implementado;

5.2.4.2. Descrição da arquitetura física e lógica de cada equipamento;

5.2.4.3. Descrição do hardware e software de cada equipamento;

5.2.4.4. Estratégias de implementação dos equipamentos;

5.2.4.5. Configuração e administração dos equipamentos;

5.2.4.6. Descrição geral da plataforma de gerência;

5.2.4.7. Diagnóstico de problemas;

5.2.4.8. Configuração de alarmes para os serviços de monitoramento;

5.2.4.9. Configuração de eventos para os serviços de monitoramento;

5.2.4.10. Configuração de rotinas de coleta de dados para monitoramento;

5.2.4.11. Gerência de desempenho e segurança;

5.2.4.12. Solução de Gerência e monitoração;

5.2.4.13. Manipulação de objetos MIB, SNMP e RMON para monitoração;

5.2.4.14. Resolução de problemas (“troubleshooting”);

5.2.4.15. Gestão de mudanças e configuração;

5.2.4.16. Relatórios de acesso;

5.2.5. A contratada deverá apresentar certificados individuais contendo carga horária, conteúdo programático, assinatura do preposto e do instrutor;

5.2.6. A passagem de conhecimento acontecerá fora das dependências da PGDF e será de responsabilidade da CONTRATADA. Deverá ser em Brasília/DF, preferencialmente perto da Sede da Procuradoria do DF, no turno vespertino, compreendido entre as 14h e 18h e para uma turma de no máximo 6 (seis) participantes;

5.2.7. A passagem de conhecimento terá seu início conforme prazo definido neste documento, e prosseguirá em dias úteis sequenciais a partir do primeiro dia de início da mesma. A critério da administração, os dias de início, término e/ou demais dias de curso poderão ser alterados, ou até mesmo serem programados para serem realizados em dias alternados, ou a metade do curso sendo ministrado antes da instalação e a outra metade após a instalação, ou da forma que melhor se adeque as necessidades da Casa, sem nenhum ônus para a PGDF;

5.2.8. Os custos referentes a deslocamento dos instrutores, se necessário, serão de responsabilidade da contratada, incluindo passagens, hospedagem, alimentação e/ou qualquer outro tipo de despesa;

5.2.9. O material didático deverá estar incluído, sem custo adicional para a PGDF. Ademais, todos os documentos utilizados para a transferência de conhecimento devem ser disponibilizados em idioma português do Brasil. Os manuais técnicos e operacionais dos softwares deverão ser disponibilizados preferencialmente em idioma português do Brasil, podendo ser língua Inglesa;

5.2.10. Ao final das transferências de conhecimento, a contratada deverá encaminhar a PGDF a relação de frequência dos participantes.

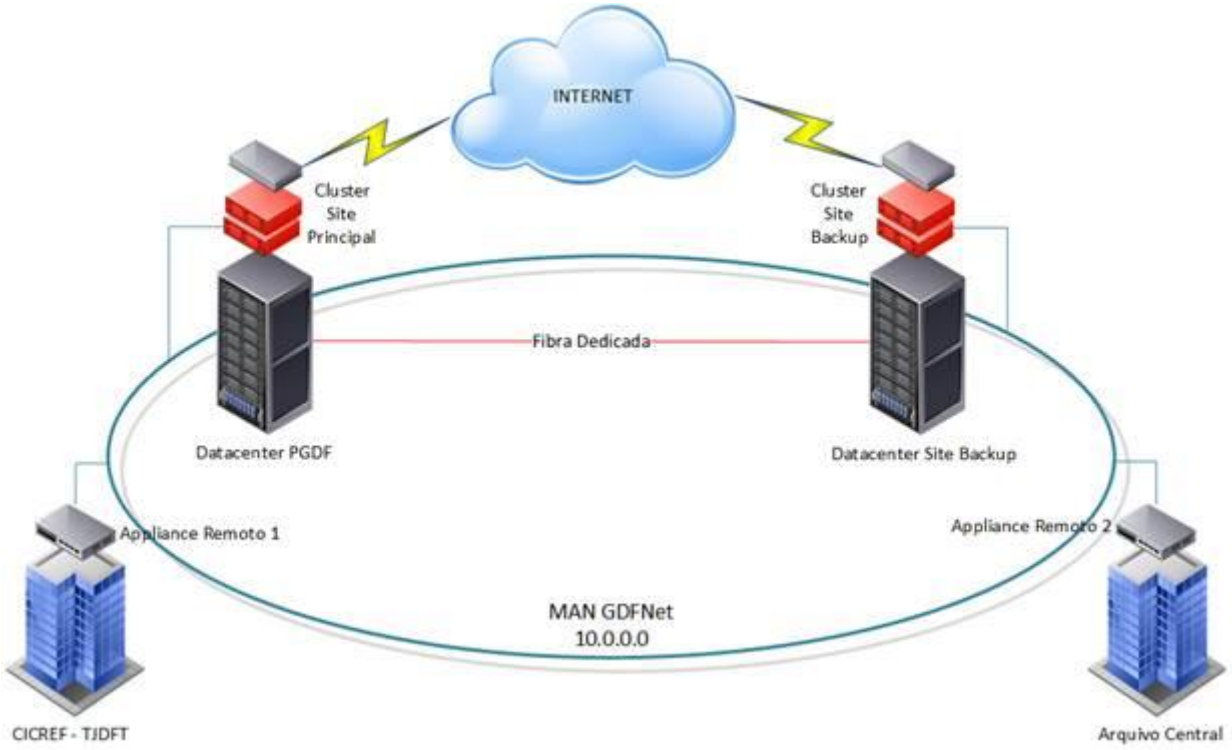
5.2.11. A PGDF reserva-se o direito de solicitar novo treinamento se o oferecido for motivo de questionamento em relação à qualidade e à carga horária efetiva;

5.3. INSTALAÇÃO E CONFIGURAÇÃO DOS EQUIPAMENTOS

5.3.1. A instalação e configuração se dará a partir do Projeto de Implantação da Solução estabelecida no tópico **"5.1 DO PROJETO DE IMPLANTAÇÃO DA SOLUÇÃO"**;

5.3.2. O ambiente a ser modificado para a instalação e configuração dos firewalls será conhecido através da vistoria às instalações da PGDF definida no tópico "**3.4 O Firewall** Appliance Tipo 1 está representado na figura adentro do ambiente do Datacenter PGDF (Cluster Site Principal), o Firewall Appliance Tipo 2 está representado na figura adentro do ambiente do Datacenter Site Backup (Cluster Site Backup) e o Firewall Appliance Tipo 3, que são departamentos da PGDF localizados em outros endereços, e estão representados na figura abaixo adentro dos ambientes da GECONFI (Prédio do TJ - Appliance Remoto 1) e do Arquivo Central (Appliance Remoto 2).

5.3.3. Nessa solução que consiste em 6 (seis) equipamentos, sendo que 4 (quatro) equipamentos deverão compor 2 (dois) clusters ativo-ativo, sendo um cluster instalado no site principal, localizado no endereço SAM Projeção I e o outro no site backup, no endereço SAM Projeção H. Os outros 2 (dois) equipamentos tem menos poder de processamento e ficarão: a) Arquivo Central; b) GECONFI, escritório localizado dentro do TJ; onde tais unidades se conectarão ao edifício sede da Procuradoria Geral do DF, conforme figura abaixo:



5.3.4. DA VISTÓRIA" e também através da reunião estabelecida no tópico **"5.1 DO PROJETO DE IMPLANTAÇÃO DA SOLUÇÃO",** ambos deste Termo de Referência;

5.3.5. A instalação e configuração dos equipamentos só poderão ser efetuadas por técnico treinado, capacitado e certificado pelo fabricante dos equipamentos;

5.3.6. O técnico a serviço da contratada deve proceder à desconexão e remoção dos equipamentos que serão substituídos existentes no rack, afixação dos novos componentes em rack existente no local, conexão às redes elétrica e lógica do local, configuração e ativação dos componentes. Deve, também, proceder à verificação das condições básicas de funcionamento, restaurando o estado operacional da rede local;

5.3.7. A instalação e ativação dos equipamentos deverá ser realizada entre 08:00h e 18:00h nos dias de expediente. A critério da administração, sem nenhum ônus para a PGDF, esse horário de instalação poderá ser ajustado para o período entre 18:00h e 24:00h nos dias de expediente e entre 8:00h e 18:00h nos finais de semanas e feriados, para que não haja qualquer prejuízo da operacionalidade da rede local nos horários de expediente;

5.3.8. Durante o período da instalação e configuração da solução, caso haja algum problema que limite os serviços de TI em decorrência da instalação e configuração, a CONTRATADA deverá comparecer ao local de instalação em no máximo 1 (uma) hora após a abertura de chamado e resolver o problema em definitivo em até no máximo 2 (duas) horas após a abertura do chamado;

5.3.9. Após a instalação e configuração dos equipamentos, os mesmos devem estar ativos em modo operacional para uso da PGDF. A instalação só se conclui quando todos os equipamentos e serviços estiverem funcionando 100% no ambiente da Procuradoria;

5.3.10. Todos os softwares instalados deverão ser disponibilizados em sua melhor configuração tecnológica (última versão e upgrade de firmware);

5.3.11. No caso de não conformidade dos componentes da solução, verificada pela PGDF, os componentes devem ser desinstalados, embalados novamente e retirados pela contratada. Os equipamentos de rede anteriormente desinstalados devem ser reinstalados e reativados do modo como foram encontrados.

5.4. DAS CONDIÇÕES DE INSTALAÇÃO E SUAS MOVIMENTAÇÕES

5.4.1. Os equipamentos deverão ser instalados nos locais indicados no subtópico **"5.6 DO LOCAL E DAS CONDIÇÕES DE EXECUÇÃO"**;

5.4.2. Em virtude de razões e necessidades internas (como por exemplo a aquisição do novo Datacenter da PGDF que acontece concomitantemente a esta aquisição), a PGDF poderá solicitar a alteração do dia e/ou do local de instalação da solução e/ou realizar movimentações desta solução de firewall para outros locais diversos de onde o mesmo foi instalado inicialmente, conforme regras abaixo:

5.4.2.1. O local de instalação da solução de Firewall no Site Backup, definida para ser realizada no Edifício Sede da CODEPLAN, poderá ser alterada a critério da administração, e com isso ser realizada no Edifício Sede da PGDF, e posteriormente, ainda durante a vigência do contrato, ser movimentada para o Edifício Sede da CODEPLAN ou para qualquer outro departamento da PGDF instalado em outras localidades dentro do DF, com todas as custas referente a movimentação, nova instalação, configuração e ativação da solução sobre responsabilidade da CONTRATADA;

5.4.2.2. A instalação da solução de Firewall nos departamentos localizados fora da SEDE da PGDF: Arquivo Geral e no GECONFI, definidas para serem realizadas na quadra 05 do SGON, e Prédio Sede do TJ, respectivamente, poderá ser alterada a critério da administração, e com isso ser realizada no Edifício Sede da PGDF, e posteriormente, ainda durante a vigência do contrato, ser movimentada para os locais previamente definidos neste termo de referência ou para qualquer outro departamento da PGDF instalado em outras localidades dentro do DF, com todas as custas referente a movimentação, nova instalação, configuração e ativação da solução sobre responsabilidade da CONTRATADA;

5.4.2.3. A instalação da solução de Firewall no Site Principal, definida para ser realizada no Edifício Sede da PGDF, poderá ser alterada a critério da administração, e com isso ser realizada em qualquer outro departamento da PGDF instalado em outras localidades dentro do DF, e posteriormente, ainda durante a vigência do contrato, ser movimentada para o NOVO Edifício Sede da PGDF ou para qualquer outro departamento da PGDF instalado em outras localidades dentro do DF, com todas as custas referente a movimentação, nova instalação, configuração e ativação da solução sobre responsabilidade da CONTRATADA;

5.4.3. A CONTRATADA, após ser comunicada da necessidade de movimentação dos equipamentos, deverá designar um técnico no prazo máximo de 5 (cinco) dias para realizar o procedimento de movimentação, e caso necessário, nova instalação, configuração e ativação da solução;

5.4.4. O não envio do técnico em tempo hábil para realização dos trabalhos será considerado como descumprimento de contrato e a CONTRATADA poderá receber sanções conforme especificado neste termo de referência e legislação vigente;

5.4.5. De forma similar, o não envio do técnico em tempo hábil para realização dos trabalhos será entendido que a CONTRATADA aceita que a movimentação poderá ser realizada pela CONTRATANTE, sem prejuízo da manutenção da garantia e suporte técnico da solução;

5.5. DA GARANTIA E SUPORTE TÉCNICO

5.5.1. O garantia e suporte técnico dos componentes da solução deverá ser realizada de forma on-site, ou seja. A garantia e suporte técnico deverá ser prestada pelo prazo mínimo de 48 (quarenta e oito) meses, contados da data do seu recebimento definitivo;

5.5.2. Os equipamentos deverão ter garantia e assistência técnica no local onde serão instalados pelo período estipulado no item anterior, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

5.5.3. Durante todo o período de garantia está incluído a atualização tecnológica de todas as licenças e softwares presentes na solução, sem nenhum ônus adicional para a PGDF;

5.5.4. O suporte técnico deve manter o equipamento sempre atualizado com a última versão do firmware, porém a atualização deverá ocorrer de forma planejada – formalizada por um plano de mudanças.

5.5.5. Independentemente da aceitação, a contratada garantirá a qualidade de cada unidade do equipamento fornecido pelo prazo estabelecido de no mínimo 48 (quarenta e oito) meses, obrigando-se a repor aquele que apresentar defeito:

5.5.5.1. Se apenas 1 (um) equipamento de cada item da solução apresentar defeito, o mesmo deverá ser trocado por outro equipamento novo, de qualidade igual ou superior, que atenda todos os requisitos estabelecidos neste Termo de Referência no prazo máximo de 30 dias;

5.5.5.2. Se 2 (dois) ou mais equipamentos de cada item apresentar defeito, os mesmos deverão ser trocados por outros equipamentos novos, de qualidade igual ou superior, que atenda todos os requisitos estabelecidos neste Termo de Referência no prazo máximo de 4 horas. Esse prazo é devido ao fato da PGDF não poder ficar sem a presente solução de segurança da informação, tal fato poderia gerar riscos incalculáveis aos ativos da Casa;

5.5.6. A contratada deverá prover uma central de atendimento gratuito ou com custo de ligação local, para realizar abertura de chamados mediante a utilização dos seguintes meios de comunicação:

5.5.6.1. Telefone: 24 horas por dia, 7 dias por semana e 365 dias por ano;

5.5.6.2. E-mail e internet: 24 horas por dia, 7 dias por semana e 365 dias por ano;

5.5.7. A central de atendimento deve possuir software na web ou enviar por e-mail o status do chamado e histórico contínuo do atendimento. Deve possuir meio para que a CONTRATANTE controle mensalmente e anualmente, dentro do período de vigência do contrato, os relatórios estatísticos, os chamados abertos, em atendimento, concluídos etc.

5.5.8. A PGDF fará a “Abertura de Chamados Técnicos” que deverão obedecer os prazos de atendimento estipulados abaixo:

Severidade	Descrição	Prazo de Solução Definitiva
ALTA	Este nível de severidade é aplicado quando há indisponibilidade no uso dos serviços.	4 (quatro) horas
MÉDIA	Este nível de severidade é aplicado quando há falha, simultânea ou não, no uso dos serviços, estando ainda disponíveis, porém apresentando problemas.	6 (seis) horas
BAIXA	Este nível de severidade é aplicado para problemas que não afetem o desempenho e	5 (cinco) dias úteis

	disponibilidade dos serviços, bem como para atualizações de software do roteador, esclarecimentos técnicos relativos ao uso e aprimoramento dos serviços. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados.	

5.5.9. Será considerado para efeitos do nível de serviço exigido, prazo de solução definitiva, como o tempo decorrido entre a abertura do chamado técnico efetuada pela equipe técnica da PGDF à CONTRATADA e a efetiva recolocação dos serviços em seu pleno estado de funcionamento e consequentemente resolução do problema;

5.5.10. Depois de concluído a resolução do chamado referente ao pedido de suporte, a CONTRATADA comunicará o fato à equipe técnica da PGDF e solicitará autorização para o fechamento do chamado. Caso a PGDF não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Neste caso, a PGDF fornecerá as pendências relativas ao chamado aberto;

5.5.11. A CONTRATADA deverá disponibilizar pelo Portal de Atendimento ou por E-mail, uma forma de acompanhamento dos serviços contratados.

5.5.12. Entende-se como Portal de Atendimento, qualquer ferramenta de gerência acessível através da Internet por intermédio de um navegador Web, com acesso restrito através de usuário/senha eletrônica.

5.5.13. O Portal de Atendimento deverá possuir informações de estatísticas do desempenho da rede, consulta aos históricos dos registros das ocorrências e registros de solicitações e reclamações enviadas pela PGDF;

5.5.14. A CONTRATADA deverá fornecer pelo menos um usuário/senha para acessar o Portal de Atendimento dos Serviços. O Portal de Atendimento poderá ser substituído pelo E-mail, conforme tópico 5.5.11;

5.5.15. Geração de relatórios online (mensal e anual) com histórico de chamados abertos pela PGDF;

5.5.16. Possuir meios de auditoria de todos os serviços, possibilitando que a PGDF possa sempre que desejar, comprovar a qualidade e eficácia dos serviços oferecidos;

5.5.17. Deverá ser fornecido mensalmente, juntamente com a Nota Fiscal, o relatório detalhado contendo todos os registros de chamados técnicos abertos no referido período;

5.5.18. Deve ser informado link (URL) de site na internet do fabricante dos equipamentos com disponibilidade de informações para suporte, tais como: guia de instalação, informações técnicas, atualização e download de drives, firmwares upgrade de BIOS.

5.6. DO LOCAL E DAS CONDIÇÕES DE EXECUÇÃO

5.6.1. Os equipamentos deverão ser entregues no Edifício Sede da Procuradoria-Geral do Distrito Federal, no endereço SAM Bloco “I” Edifício Sede Asa Norte;

5.6.2. Os serviços de instalação e configuração como a garantia e suporte técnico a serem prestados deverão ser realizados no âmbito do parque tecnológico do Edifício Sede da Procuradoria-Geral do Distrito Federal, no endereço SAM Bloco “I” Edifício Sede Asa Norte, onde se encontra o site principal; no Edifício Sede da CODEPLAN, no endereço SAM, Projeção H, Asa Norte, onde se encontra o site backup; no Arquivo Geral da PGDF, no endereço SGON, quadra 05 lote 23, área

especial; na GECONFI, localizada no prédio do TJDF; e também em outros departamentos da PGDF instalados em outras localidades dentro do DF, caso venha a surgir;

5.6.3. Quando o serviço de instalação for realizado fora do edifício sede da Procuradoria, a CONTRATADA ficará responsável por pegar os equipamentos na sede da PGDF (ou nos departamentos da PGDF dentro do DF) e levá-los até o local indicado para a instalação e assim realizar toda a configuração e ativação da solução;

5.6.4. Todos os equipamentos fornecidos e seus componentes deverão ser novos, em linha de produção e de primeiro uso, entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em embalagens originais e acompanhados de todos os acessórios, cabos, conectores, kits de fixação, fibras óticas (incluindo fusão, se necessário) *patchcords*, etc, necessários às suas instalações, ativação e operação, onde serão recebidos provisoriamente para que seja verificado se suas características atendem ao especificado neste edital e na proposta da Licitante;

5.6.5. A CONTRATADA deverá instalar o equipamento e seus componentes no local indicado pela PGDF, incluindo o material, mão-de-obra, ferramental, sem ônus adicional para a Contratante ou prejuízo para seus serviços;

5.6.6. A CONTRATADA deverá configurar o equipamento de acordo com o padrão já utilizado pela rede local da PGDF, como também deverá garantir a plena operação do equipamento instalado em harmonia com os demais e de acordo com as regras já definidas para a rede local da PGDF.

6. ELEMENTOS PARA GESTÃO DO CONTRATO

6.1. OBRIGAÇÕES DO CONTRATANTE

6.1.1. Acompanhar, fiscalizar e conferir o objeto contratual;

6.1.2. Proporcionar todas as facilidades para que a CONTRATADA possa efetuar os serviços dentro das normas estabelecidas no contrato;

6.1.3. Permitir livre acesso aos funcionários da CONTRATADA aos equipamentos, objeto deste contrato, para execução dos serviços de instalação, configuração, garantia e suporte técnico;

6.1.4. Receber os equipamentos e serviços entregues pela CONTRATADA, desde que estejam em conformidade com o objeto contratado;

6.1.5. Prestar informações e esclarecimentos que venham a ser solicitados pela CONTRATADA;

6.1.6. Notificar à CONTRATADA sobre imperfeições, falhas ou irregularidades constatadas nos equipamentos e serviços, para que sejam adotadas as medidas necessárias;

6.1.7. Solicitar de imediato a pronta reparação, substituição de equipamentos ou qualidade do objeto contratado, ou parte, que se apresente com defeito ou em desacordo com a especificação descrita em contrato;

6.1.8. Efetuar os pagamentos devidos nos prazos previstos.

6.2. OBRIGAÇÕES DA CONTRATADA

6.2.1. Cumprir fielmente as obrigações assumidas constantes do Edital de Licitação, do Contrato e da Proposta, de forma que os serviços sejam realizados com esmero e perfeição;

6.2.2. Fornecer por sua conta e responsabilidade os equipamentos, softwares, licenças (e qualquer outro material necessário para a configuração e ativação da solução), serviços de instalação, configuração

e passagem de conhecimento necessários ao funcionamento e operação da solução, bem como fornecer o serviço de garantia e assistência técnica, conforme as especificações, níveis de qualidade e prazos contratados, e assim mantê-los por todo o período de garantia;

6.2.3. Reunir-se com a PGDF para levantar as necessidades de projeto de acordo com os prazos e regras definidas neste Termo de Referência e seus anexos;

6.2.4. Entregar o projeto de implantação da solução de acordo com os prazos e regras definidas neste Termo de Referência e seus anexos;

6.2.5. Realizar a instalação e configuração dos equipamentos conforme especificações contidas neste Termo de Referência e seus anexos;

6.2.6. Realizar as movimentações dos equipamentos conforme prazos e especificações contidas neste Termo de Referência e seus anexos;

6.2.7. Efetuar transferência de conhecimento para os colaboradores indicados pela Diretoria de Organização e Sistemas (DISIS) de modo que eles sejam capazes de configurar e operar o equipamento e conforme especificações deste Termo de Referência e seus anexos;

6.2.8. Cumprir os prazos de resolução de chamados definidos para a fase de instalação e configuração da solução;

6.2.9. Cumprir os prazos de resolução de chamados definidos para a fase de garantia e suporte técnico da solução;

6.2.10. Apresentar comprovação de que empresa possui em seu corpo técnico, pelo menos 01 (um) técnico com certificação oficial fornecida pelo(s) fabricante(s) dos produtos o qual deverá compor a equipe que irá realizar o projeto de implantação, realizar a instalação e configuração da solução contratada e prestar o suporte técnico necessário. A comprovação do vínculo do profissional com a licitante poderá ser feito por meio de contrato social ou equivalente, carteira de trabalho ou contrato de prestação de serviços, sem vínculo trabalhista e regido pela legislação civil comum.

6.2.11. Os equipamentos disponibilizados a CONTRATANTE deverão ser novos, de primeiro uso e estar na linha atual de produção do fabricante;

6.2.12. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas (sem quaisquer ônus para a PGDF), no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados (art.69 da Lei nº 8.666/93);

6.2.13. Assumir todos os gastos e despesas que fizer, para o adimplemento das obrigações decorrentes do Contrato;

6.2.14. Manter, em compatibilidade com as obrigações por ela assumidas, durante toda a vigência do contrato, todas as condições de habilitação e qualificação exigidas na licitação;

6.2.15. Providenciar junto à PGDF a identificação dos seus empregados, os quais deverão porta-se adequadamente nas dependências da PGDF;

6.2.16. Responder por todos os encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução do objeto contratado, vez que seus empregados não terão qualquer vínculo empregatício com a CONTRATANTE;

6.2.17. Não causar qualquer dano à estrutura física da PGDF;

6.2.18. Ressarcir ao Contratante quaisquer danos ou prejuízos causados à Administração em decorrência da execução dos serviços.

6.2.19. Não transferir a terceiro, por qualquer forma, nem mesmo parcialmente, o contrato;

6.2.20. A CONTRATADA deverá assinar TERMO DE CONFIDENCIALIDADE e manter sigilo de todos os dados ou informações da CONTRATANTE ou de suas representações obtidas em função da prestação do serviço contratado, conforme definido no subtópico "**6.8 DO SIGILO"**;

6.2.21. Obriga-se a aceitar, nas mesmas condições contratuais, e mediante Termo Aditivo, os acréscimos ou supressões que se fizerem necessários, no montante de até 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato, de acordo com os Parágrafos Primeiro e Segundo do Artigo 65 da Lei nº 8.666/93.

6.2.22. As funcionalidades do firewall, de IPS, antivírus e *anti-spyware* devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

6.3. DA VIGÊNCIA DO CONTRATO

6.3.1. A vigência do contrato é de 51 (cinquenta e um) meses, a contar da data da assinatura do contrato, em face dos prazos de entrega dos equipamentos, de procedimentos de recebimento fixados, da instalação e configuração da solução, passagem de conhecimento, bem como da garantia, onde neste caso, iniciar-se-á a contagem a partir do recebimento definitivo da solução, conforme estabelecido no subtópico **"5.5 DA GARANTIA E SUPORTE TÉCNICO"**.

6.4. ACOMPANHAMENTO DO CONTRATO

6.4.1. O acompanhamento do contrato será aferido através dos seguintes eventos:

a. Entrega dos bens X Conformidade com as especificações do edital;
b. Instalação e configuração X Solução do firewall em funcionamento;
c. Passagem de conhecimento X Questionamentos em relação à qualidade e à carga horária;
d. Assistência técnica em garantia X Disponibilidade do canal e tempo de resolução;

6.5. DOS PRAZOS E CONDIÇÕES

6.5.1. Da Entrega dos Equipamentos

6.5.1.1. **Até 45 (quarenta e cinco) dias corridos** após a assinatura do contrato. No caso da LICITANTE prever, em sua proposta, prazo de entrega inferior a 45 dias, este último será considerado como prazo máximo para entrega dos equipamentos;

6.5.2. Do Projeto de Implantação da Solução

6.5.2.1. A LICITANTE deverá se reunir com a CONTRATANTE, nas dependências da PGDF, em até **no máximo 10 (dez) dias corridos** após a assinatura do contrato para o levantamento das necessidades do projeto com vistas a subsidiar a elaboração de um Projeto de Implantação da Solução;

6.5.2.2. A LICITANTE deverá entregar uma proposta de Projeto de Implantação da Solução em até no **máximo 30 (trinta) dias** corridos após a assinatura do contrato;

6.5.3. Da Passagem de Conhecimento

6.5.3.1. Terá início em até 30 (trinta) dias corridos após a assinatura do contrato;

6.5.4. Da Instalação e Configuração

6.5.4.1. Até 20 (vinte) dias corridos após a solicitação formal da PGDF feita através de Ordem de Serviço;

6.6. DO RECEBIMENTO PROVISÓRIO E DEFINITIVO

6.6.1. O serviço objeto da presente licitação será recebido das seguintes formas:

6.6.2. Provisória, mediante recibo, em até 5 (cinco) dias úteis após concluída as seguintes etapas: Entrega dos equipamentos da solução firewall appliances; Entrega do sistema de gerencia e monitoramento; Instalação, configuração e ativação da solução com perfeito funcionamento dos serviços; Passagem de Conhecimento; e Entrega de documento com as informações para utilização da garantia e suporte técnico;

6.6.3. Definitiva, mediante recibo, em até 10 (dez) dias úteis a partir do recebimento provisório, após comprovação da perfeita execução do serviço prestado nos termos contratuais, ocasião em que se fará constar a atestação da nota fiscal;

6.6.4. Os aceites provisórios e definitivos deverão ser elaborados de acordo com os modelos definidos no ANEXO VIII – MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO e ANEXO IX – MODELO DE TERMO DE RECEBIMENTO DEFINITIVO, respectivamente;

6.6.5. Os serviços executados em desconformidade com o especificado no instrumento convocatório ou em desacordo com as normas legais e/ou correlatas, serão rejeitados parcial ou totalmente, conforme o caso, e a Contratada será obrigada a refazê-los no prazo estipulado pela Fiscalização, contado da data do recebimento de notificação escrita, necessariamente acompanhada do Termo de Recusa, sob pena de incorrer em atraso quanto ao prazo de execução;

6.6.6. Essa notificação interrompe os prazos de recebimento e de pagamento até que a irregularidade seja sanada;

6.6.7. O aceite provisório ou definitivo não modifica, restringe ou elide a plena responsabilidade da Contratada de prestar os serviços de acordo com as especificações, quantidades e condições estabelecidas, inclusive na proposta de preços, nem invalida qualquer reclamação que o Contratante venha a fazer em virtude de posterior constatação de serviço fora de especificação, garantido o devido reparo, sem custo adicional ao Contratante.

6.7. DO PAGAMENTO

6.7.1. O pagamento da solução de segurança da informação (*firewalls appliance*s, sistema de gerencia e monitoração, serviços de instalação e configuração, passagem de conhecimento) será realizado de uma única vez, mediante apresentação do Termo de Recebimento Definitivo da Solução, emitido e assinado pelo gestor do contrato, no prazo de até 30 (trinta) dias após a entrega da nota Fiscal/Fatura;

6.7.2. O pagamento do serviço de suporte técnico em garantia on-site será feito mensalmente, somente após o recebimento definitivo da solução, mediante atesto do gestor do contrato, comprovando o perfeito funcionamento da solução e prestação do serviço de suporte técnico, além da Nota Fiscal/Fatura referente a estes serviços prestados, bem como do relatório detalhado de serviço estabelecido no subtópico 5.5.17;

6.7.3. O pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal / Fatura.

6.7.4. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, a respectiva Nota Fiscal/Fatura será restituída à Contratada para as correções necessárias e o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

6.7.5. Para efeito de pagamento, a CONTRATADA deverá apresentar os documentos estabelecidos no Edital.

6.8. DO SIGILO

6.8.1. A PGDF e a empresa contratada assumem mútuas obrigações de sigilo. A CONTRATADA deve manter sigilo de todos os dados ou informações da CONTRATANTE ou de suas representações obtidas em função da prestação do serviço contratado.

6.8.2. A Contratada deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do Contratante, devendo orientar seus empregados e/ou prepostos nesse sentido, sob pena de responsabilidade civil, penal e administrativa;

6.8.3. Para formalização da confidencialidade exigida, a CONTRATADA deverá assinar Termo de Confidencialidade sobre Segurança da Informação, conforme ANEXO VII – MODELO DE TERMO DE CONFIDENCIALIDADE, comprometendo-se a respeitar todas as obrigações relacionadas com confidencialidade e segurança das informações pertencentes à CONTRATANTE, mediante ações ou omissões, intencionais ou acidentais, que impliquem na divulgação, perda, destruição, inserção, cópia, acesso ou alterações indevidas, independentemente do meio no qual estejam armazenadas, em que trafeguem ou do ambiente em que estejam sendo processadas;

6.8.4. O Termo mencionado no item anterior será assinado pelo representante da CONTRATADA, que deverá dar ciência aos profissionais envolvidos na prestação do serviço, sendo entregue no ato da assinatura do contrato;

6.9. MECANISMOS FORMAIS DE COMUNICAÇÃO

6.9.1. Quaisquer questões administrativas durante a execução do contrato, de cunho mais formal:

a. Emissor: PGDF / Empresa Contratada.
b. Destinatário: PGDF / Empresa Contratada.
c. Forma de Comunicação: Correio.
d. Documento: Ofício.
e. Periodicidade: Eventual.

6.9.2. Questões administrativas cotidianas durante a execução do contrato:

a. Emissor: PGDF / Empresa Contratada.
b. Destinatário: PGDF / Empresa Contratada.
c. Forma de Comunicação: E-mail.
d. Documento: Mensagem eletrônica.
e. Periodicidade: Eventual.

6.9.3. Abertura de Chamados:

a. Emissor: PGDF.
b. Destinatário: Empresa Contratada.
c. Forma de Comunicação: E-mail, telefone (com custo de ligação local) ou página web (com retorno do número do chamado).
d. Documento: Mensagem eletrônica ou ligação telefônica.

e. Periodicidade: Eventual, no período de 24 x 7 (vinte e quatro horas por dia x sete dias por semana).

6.9.4. Prestação do suporte técnico em garantia:

a. Emissor: Empresa contratada.

b. Destinatário: PGDF.

c. Forma de Comunicação: Pessoalmente na sede da PGDF.

d. Periodicidade: Eventual, no período de 24 x 7 (vinte e quatro horas por dia x sete dias por semana).

6.9.5. Apresentação dos serviços prestados com vistas a sua avaliação / Entrega de relatórios

a. Emissor: Empresa contratada.

b. Destinatário: PGDF.

c. Forma de Comunicação: Deverá ser entregue junto com a Nota Fiscal (Deverá também estar disponível no Portal de Atendimento).

d. Periodicidade: Eventual / Mensal.

e. Documento: Relatórios.

7. MODELO DE PROPOSTA E ESTIMATIVA

7.1. MODELO DE PROPOSTA

7.1.1. Deverá vir acompanhada de documento(s) contendo a especificação técnica detalhada dos produtos cotados; e

7.1.2. Deverá vir acompanhada da comprovação de todas as características técnicas obrigatórias, que deverão ser do fabricante e comprovadas por meio de folders, catálogos, manuais, *datasheets*, *partnumbers*, ou impressão de páginas do fabricante na Internet, os quais deverão demonstrar, com exatidão, o atendimento aos itens especificados no ANEXO I.1 – CARACTERÍSTICAS TÉCNICAS MÍNIMAS OBRIGATÓRIAS.

7.1.3. A proposta deverá ser elaborada observando o modelo constante do ANEXO III – MODELO DE PROPOSTA.

7.1.4. A PGDF poderá fazer diligências/consultas no sentido de sanar dúvidas quanto ao atendimento das especificações relativas a solução e aos equipamentos ofertados.

7.2. VALOR ESTIMADO

7.2.1. Para o valor máximo, vide ANEXO II – ESTIMATIVA DE CUSTOS.

8. SANÇÕES APLICÁVEIS

8.1. As multas deverão ser aplicadas à CONTRATADA, em caso de descumprimento das cláusulas, conforme planilha abaixo:

TABELA 1 - PERCENTAGEM	
GRAU	%
1	0,025
2	0,030

3	0,10
4	0,25
5	0,50
6	0,75
7	1,0
8	1,1

TABELA 2 – INFRAÇÃO/GRADUAÇÃO		
N.	**INFRAÇÃO**	GRAU
1	**Descrição:** Descumprimento do prazo de entrega dos equipamentos, conforme estabelecido no subtópico "6.5.1 Da Entrega dos Equipamentos". **Unidade Temporal:** % por dia, limitado a 15 (quinze) dias de atraso. **Correspondência:** sobre o valor dos equipamentos.	3
2	Descumprimento do prazo de reunião com a PGDF afim de levantar as necessidades de projeto para subsidiar a elaboração do projeto de implantação da solução, conforme prazo estabelecido no subtópico "6.5.2 Do Projeto de Implantação da Solução". **Unidade Temporal:** % por dia, limitado a 15 (quinze) dias de atraso. **Correspondência:** sobre o valor da instalação e configuração da solução.	4
3	Descumprimento do prazo de entrega do projeto de implantação da solução, conforme prazo estabelecido no subtópico "6.5.2 Do Projeto de Implantação da Solução". **Unidade Temporal:** % por dia, limitado a 15 (quinze) dias de atraso. **Correspondência:** sobre o valor da instalação e configuração da solução.	6
4	Descumprimento do prazo de início da passagem de conhecimento, conforme estabelecido no subtópico "6.5.3 Da Passagem de Conhecimento"; **Unidade Temporal:** % por dia, limitado a 20 (vinte) dias de atraso. **Correspondência:** sobre o valor da passagem de conhecimento da solução.	8
5	Descumprimento do prazo de instalação e configuração da solução, conforme estabelecido no subtópico "6.5.4 Da Instalação e	7

	Configuração". **Unidade Temporal:** % por dia, limitado a 15 (quinze) dias de atraso. **Correspondência:** sobre o valor da instalação e configuração da solução.	
6	Descumprimento do prazo de movimentação e sua respectiva reinstalação (caso precise) dos equipamentos, conforme estabelecido no subtópico "5.4.3". **Unidade Temporal:** % por dia, limitado a 20 (vinte) dias de atraso. **Correspondência:** sobre o valor da instalação e configuração da solução.	5
7	Descumprimento do prazo de atendimento de suporte técnico, conforme estabelecido no tópico "5.5 Da Garantia e Suporte Técnico", na resolução do problema. **Unidade Temporal:** % por hora, limitado à 48 (quarenta e oito) horas de atraso. **Correspondência:** sobre o valor total do contrato.	1
8	Descumprimento dos prazos de entrega de relatório mensal, conforme estabelecido no subtópico "5.5.17"; **Unidade Temporal:** % por dia, limitado à 15 (quinze) dias de atraso. **Correspondência:** sobre o valor total do contrato;	2

8.2. Para fins de comprovação de tempo para aplicação das multas referente às infrações de número 7, considera-se como 1 (uma) hora inteira a fração igual ou superior 30 minutos;

8.3. Ademais, sem prejuízo com as sanções definidas acima, caso a CONTRATADA não cumpra integralmente as obrigações assumidas, garantida a prévia defesa, fica sujeita as sanções previstas no Decreto nº 26.851, de 30 de maio de 2006, e alterado pelos Decretos nºs 26.993/2006 e 27.069/2006, decreto nº 26.851 que regulamenta a aplicação das sanções administrativas previstas nas Leis Federais 8.666/93 e 10.520/2002, segue breve descrição abaixo e os detalhes estão na legislação informada acima:

a. Advertência por escrito quando do descumprimento de qualquer um dos requisitos constantes deste termo de referência;
b. Multa, conforme percentuais definido no Decreto nº 26.851 e suas atualizações;
c. Suspensão temporária de participação em licitação, e impedimento de contratar com a Administração do Distrito Federal, por prazo não superior a 2 (dois) anos, e dosada segundo a natureza e gravidade da falta cometida;
d. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos que determinaram sua punição ou até que seja promovida sua reabilitação perante a própria autoridade.
e. Caso haja aplicação de multa, o valor será descontado de qualquer fatura ou crédito existente na CONTRATADA em favor do futuro contratado ou na execução da garantia prestada. Caso a mesma seja superior ao crédito eventualmente existente, a diferença será cobrada administrativa ou judicialmente, se necessário.

8.4. Outras sanções poderão ser impostas à CONTRATADA conforme fixadas na Minuta do Contrato;

9. Critérios de Seleção de Fornecedor

9.1. QUALIFICAÇÃO TÉCNICA.

9.1.1. Apresentar pelo menos um Atestado *de* Capacidade Técnica (declaração ou certidão), em nome da licitante, fornecido por Pessoa Jurídica de Direito Público ou Privado, declarando ter a empresa licitante fornecido e implantado solução de proteção de segurança de informação composta por pelos menos 2 (dois) firewalls *appliance*, operando em cluster ativo/ativo, em uma rede local com no mínimo 400 (quatrocentos) usuários;

9.1.2. Apresentar comprovação ponto a ponto, por escrito, por meio de documentação oficial do fabricante, do atendimento as especificações mínimas dos produtos, dos seguintes itens/tópicos do Anexo I.1: 1.6.1.1 a 1.6.1.3, 1.6.1.6, 1.6.1.12, 1.6.1.18 a 1.6.1.22, 1.6.2.2, 1.6.2.4, 1.6.2.5, 1.6.2.8 a 1.6.2.12, 1.6.3.1.1 a 1.6.3.1.22, 1.6.4.1, 1.6.4.3, 1.6.4.5, 1.6.4.8, 1.6.4.12 a 1.6.4.19, 1.6.4.22 a 1.6.4.32, 1.6.5.2 a 1.6.5.8, 1.6.5.10, 1.6.5.12 a 1.6.5.14, 1.6.6.1.2 a 1.6.6.1.11, 1.6.7.1 a 1.6.7.6, 1.6.8.1 a 1.6.8.7, 1.6.9.1 a 1.6.9.7, 1.6.10.1, 1.6.11.1 a 1.6.11.9, 1.6.12.1, 1.6.12.3, 1.6.12.5 a 1.6.12.11, 1.6.12.13, 1.6.12.15 a 1.6.12.18, 1.7.1.1, 1.7.1.2, 1.7.1.6 a 1.7.1.9, 1.7.2.1, 1.7.2.4, 1.7.2.5 a 1.7.2.10, 1.7.2.12 a 1.7.2.21, 1.7.3.1 a 1.7.3.11, 1.7.4.1.3 a 1.7.4.1.10, 1.7.4.1.12, 1.7.4.1.16, 1.7.4.1.19 a 1.7.4.1.21, 1.7.5.1 a 1.7.5.6, 1.7.6.1, 1.7.6.3, 1.7.6.10 a 1.7.6.14, 1.7.6.20 a 1.7.6.23. Deverá ser apresentado conforme modelo do ANEXO IV – "MODELO DE COMPROVAÇÃO PONTUAL DE ATENDIMENTO À ESPECIFICAÇÃO TÉCNICA";

9.1.3. A aprovação da COMPROVAÇÃO PONTUAL DE ATENDIMENTO À ESPECIFICAÇÃO TÉCNICA, suportado pela Equipe Técnica, é condição necessária para a adjudicação do vencedor da licitação.

9.1.4. Os Manuais técnicos, os atestados de capacidade técnica, bem como os documentos citados na comprovação ponto-a-ponto devem ser preferencialmente em português, mas poderão ser aceitos, excepcionalmente, em língua inglesa, caso não haja a documentação escrita em língua portuguesa.

9.1.5. Todos os componentes necessários ao perfeito funcionamento de cada um dos SUBITENS do objeto devem estar discriminados e precificados na proposta.

9.1.6. Qualquer item adicional à Planilha de Formação de Preço, que vier a ser necessário para garantir o perfeito funcionamento, quando ocorrer a implantação em campo, será de total responsabilidade da CONTRATADA, não cabendo ônus algum a PGDF.

9.1.7. Apresentar juntamente com a Proposta de Preços toda documentação necessária para subsidiar o julgamento técnico das soluções ofertadas para atendimento das funcionalidades descritas neste Termo de Referência;

9.1.8. A PGDF poderá fazer diligências/consultas no sentido de sanar dúvidas quanto ao atendimento das especificações relativas aos equipamentos ofertados.

9.2. CRITÉRIOS DE ACEITABILIDADE DE PREÇOS.

9.2.1. Os preços devem ser compatíveis com os preços praticados na Administração Pública, de acordo com o Art. nº 15, Inciso V da Lei 8.666/93, a qual diz que as compras sempre que possível, deverão balizar-se pelos preços praticados no âmbito dos órgãos e entidades da Administração Pública. Os preços não poderão ser superiores aos valores constantes da Estimativa de Custos.

9.2.2. O VALOR TOTAL DA PROPOSTA É CONSTITUÍDO PELO VALOR TOTAL DO ITEM.

9.2.3. **Critérios de julgamento**

9.2.3.1. MENOR PREÇO GLOBAL PARA O ITEM.

10. DA PROVA DE CONCEITO

10.1. A PGDF solicitará amostra do produto ofertado para realização de prova de conceito, previamente à adjudicação, com o intuito de sanar dúvidas e comprovar as funcionalidades e requisitos técnicos da solução.

10.2. O objetivo é comprovar tecnicamente, juntamente com a documentação do fabricante, se a solução de firewall *appliance* (equipamentos, licenças e softwares) de fato atende aos requisitos constantes nas especificações técnicas.

10.3. A LICITANTE classificada em primeiro lugar deverá entregar caderno de testes apresentando como serão realizados os testes e quais equipamentos, licenças, softwares e demais componentes da solução serão usados na realização dos testes de comprovação técnica, no prazo máximo de 5 (cinco) dias úteis contados a partir da solicitação da PGDF, que reserva-se o direito de solicitar ajustes no caderno de testes, que devem ser realizados no prazo de 2(dois) dias úteis pela LICITANTE.

10.4. A LICITANTE deverá disponibilizar para a realização da Prova de Conceito, no prazo de até 10 (dez) dias úteis, contados a partir do aceite do caderno de testes, todos os equipamentos, licenças, softwares e demais componentes da solução para a realização dos testes de comprovação técnica. Inclui nesse prazo a instalação dos equipamentos e componentes da solução de tal forma que fique apta para início dos testes de comprovação das funcionalidades.

10.5. A Prova de Conceito (também chamada de testes de comprovação técnica) deverão ser realizados no ambiente da LICITANTE, onde todas as despesas decorrentes com a realização dos testes são de responsabilidade da LICITANTE ofertante do melhor lance.

10.6. A LICITANTE deverá demonstrar as funcionalidades requeridas na comprovação pontual (itens especificados no subtópico 9.1.2) e algum outro que a PGDF julgar importante, no prazo máximo de 5 (cinco) dias úteis, contados a partir do início dos testes de comprovação técnica.

10.7. A equipe técnica da PGDF participará de todos os testes de comprovação das funcionalidades;

10.8. Será permitido o acompanhamento dos testes pelos outros participantes do processo licitatório ou qualquer interessado, desde que se registrem previamente para tanto, junto a Procuradoria, com antecedência de até 1 (um) dia útil do início dos testes, devendo os mesmos permanecer na condição de ouvinte, ou seja, não será permitido qualquer tipo de interferência nos testes. O acompanhamento dos testes ficará limitado a 1 (um) representante de cada participante da licitação, o qual deverá arcar com os respectivos custos de transporte e hospedagem.

10.9. A LICITANTE deve disponibilizar em até 2 (dois) dias úteis, contados a partir do fim da realização da prova de conceito, o relatório com todas as informações e resultados apurados durante os testes. Tal relatório deve constar, minimamente: informações da topologia física e lógica do ambiente utilizado, arquivos e scripts de configuração, versões de software utilizadas e registro dos logs com todas as evidências capturadas. Tais informações devem ser disponibilizadas também em meio digital.

10.10. A PGDF emitirá no prazo de até 5 (cinco) dias úteis após a entrega do relatório, o resultado da avaliação da prova de conceito. O resultado informará se os testes estão ou não de acordo com as especificações técnicas constantes neste documento;

10.11. Poderá implicar a desclassificação da proposta da LICITANTE:

10.11.1. Atendimento parcial ou não atendimento aos requisitos funcionais e de desempenho mínimos exigidos neste termo;

10.11.2. Inoperância, funcionamento irregular ou parcial das funcionalidades nos testes de laboratório;

10.11.3. Características de funcionamento que possam implicar em riscos à continuidade operacional da solução, como instabilidade ou elevação do processamento do ativo de forma desproporcional às implementações ativas.

10.11.4. Não cumprimento dos prazos estabelecidos.

10.12. Caso seja desclassificada a proposta da LICITANTE, serão convocadas as LICITANTES remanescentes, de acordo com a ordem de classificação, para realizar a Prova de Conceito, conforme regras e prazos estabelecidos acima, e após a análise de sua proposta, conforme previsto no item XI do Edital.

ANEXO I.1

CARACTERÍSTICAS TÉCNICAS MÍNIMAS OBRIGATÓRIAS

1. SOLUÇÃO DE FIREWALL

1.1. A presente contratação contempla o fornecimento, instalação, configuração, transferência de conhecimento, garantia e suporte técnico on-site de solução de segurança de rede, composta por 6 (seis) firewalls *appliances*.

1.2. Desse total, 4 (quatro) equipamentos deverão compor 2 (dois) *clusters* ativo-ativo, sendo um *cluster* instalado no site principal, localizado no endereço SAM Projeção I e o outro no site backup, no endereço SAM Projeção H. Os outros 2 (dois) equipamentos, com menor poder de processamento, conectarão os escritórios remotos do Arquivo Central e do GECONFI (dentro do TJ) ao edifício sede da Procuradoria Geral do DF, conforme o subtópico **"3.3 DA ARQUITETURA"** deste Termo de Referência.

1.3. ***Os 6 (seis) firewalls deverão ser em appliance, do mesmo fabricante, ou seja, hardware e software customizados e dedicados especificamente para a aplicação a que se destinam. Deverá vir acompanhado ao firewall todas as licenças, softwares, sistemas e/ou qualquer outro item necessário ao perfeito funcionamento dos equipamentos, bem como a garantia e suporte técnico durante 48 (quarenta e oito) meses. Não serão aceitas soluções baseadas em sistemas operacionais de uso geral, tais como UNIX, Microsoft Windows, Linux, MacOS, entre outros;***

1.4. Os *clusters* deverão operar no modo ativo-ativo. A transição entre as unidades do cluster deve ser automática, sem a perda de nenhuma conexão ativa, transparente para o usuário, ou seja, sem intervenção manual. Além disso, os componentes do cluster deverão operar sincronizados de tal forma que qualquer modificação feita na configuração do equipamento ativo será replicada imediatamente para o outro equipamento também ativo, sem nenhum tipo de interrupção no funcionamento;

1.5. O Firewall Appliance Tipo 1 está representado no ambiente do Datacenter PGDF (Cluster Site Principal), o Firewall Appliance Tipo 2 está representado no ambiente do Datacenter Site Backup (Cluster Site Backup) e o Firewall Appliance Tipo 3 está representado nos ambientes do GECONFI (Appliance Remoto 1) e do Arquivo Central (Appliance Remoto 2).

1.6. CARACTERÍSTICAS ESPECÍFICAS PARA OS 4 (QUATROS) APPLIANCES QUE COMPORÃO O CLUSTER DO SITE PRINCIPAL E DO SITE BACKUP:

1.6.1. CAPACIDADE E QUANTIDADE

1.6.1.1. Os equipamentos que comporão o cluster do Site Backup (Firewall Appliance Tipo 2) deverão possuir um *throughput* mínimo de 2 (dois) Gbps para as funcionalidades de firewall com controle de aplicação habilitado e *throughput* mínimo de 1 (um) Gbps para controle de aplicativos, IPS, antivírus e anti-spyware habilitados e atuantes simultaneamente para todas as assinaturas que o fabricante possuir;

1.6.1.2. Os equipamentos que comporão o cluster do Site Principal (Firewall Appliance Tipo 1) deverão possuir um *throughput* mínimo de 4 (quatro) Gbps para as funcionalidades de *firewall* com controle de aplicação habilitado e *throughput* mínimo de 2 (dois) Gbps para controle de aplicativos, IPS, *antivírus* e *anti-spyware* habilitados e atuantes simultaneamente para todas as assinaturas que o fabricante possuir;

1.6.1.3. Os *appliances* ofertados deverão possuir em validade a certificação *Common Criteria EAL-4* ou *ICSA Labs* (firewall);

1.6.1.4. O cluster do site backup deverá suportar, no mínimo, 250.000 (duzentas e cinquenta mil) sessões concorrentes e 50.000 (cinquenta mil) novas conexões por segundo, por equipamento;

1.6.1.5. O cluster do site principal deverá suportar, no mínimo, 500.000 (quinhentas mil) sessões concorrentes e 50.000 (cinquenta mil) novas conexões por segundo, por equipamento;

1.6.1.6. Os equipamentos fornecidos deverão possuir características de *Next Generation Firewall* (NGFW) com as seguintes funcionalidades instaladas: filtro de pacotes, controle de aplicações, NAT, PAT, IPS, *antivírus*, *anti-spyware*, IDS, DLP (*Data Loss Prevention*), IPSec VPN *site-to-site* e cliente-to-site, filtro de URL, QoS e roteamento avançado;

1.6.1.7. Fonte de alimentação 100-240VAC;

1.6.1.8. Cada *appliance* deverá possuir, no mínimo, 8 (oito) interfaces ethernet 10/100/1000 e 4 (quatro) interfaces gigabit SFP com *transceiver* compatível com a infraestrutura da PGDF, de tal forma que o tráfego de sincronismo entre os nós do *cluster* não seja exclusivo em qualquer das portas;

1.6.1.9. Possuir 1 (uma) interface ethernet dedicada para gerenciamento e monitoramento;

1.6.1.10. Possuir 1 (uma) interface do tipo console ou similar;

1.6.1.11. Suporte a, no mínimo, 10 (dez) roteadores virtuais;

1.6.1.12. Deve permitir 1.000 (um mil) clientes VPN SSL simultâneos sem a necessidade de licenças adicionais;

1.6.1.13. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para seu funcionamento;

1.6.1.14. Por console de gerência e monitoramento, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado ou appliances virtual para o funcionamento das mesmas;

1.6.1.15. A console de gerência e monitoramento podem residir no mesmo *appliance*, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;

1.6.1.16. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de *end-of-life* ou *end-of-sale*;

1.6.1.17. As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos *appliance*s, desde que obedeçam a todos os requisitos desta especificação;

1.6.1.18. A plataforma deve fazer análise de conteúdo de aplicações em camada 7 do modelo OSI;

1.6.1.19. Agregação de links 802.3ad;

1.6.1.20. Permitir a definição de políticas e/ou regras de filtragem baseadas em endereços IP, range, subnets, países, portas, protocolo, aplicação, categoria de aplicações, usuários, grupos, tipos de arquivos (tais como, mas não limitado a: exe, dll, bat, cab, pif, reg) e mecanismos de QoS (*traffic shaping, diffserv marking,* inclusive por aplicação);

1.6.1.21. Identificar e controlar o acesso dos usuários às aplicações utilizando: endereço IP, LDAP, Microsoft Active Directory, RADIUS, Kerberos, eDirectory. Os esquemas de autenticação deverão ser suportados pelos módulos de firewall (incluindo o controle de aplicações, DLP, filtros de conteúdo, IPS, *antivírus*, *anti-spyware*, QoS, roteamento baseado em políticas PBF ou PBR) e VPN. Deverá também possuir uma base de dados local para permitir a autenticação de usuários sem a necessidade de um dispositivo externo;

1.6.1.22. As funcionalidades de SSL *decryption*, VPN IPSec e SSL, controle de aplicações, QoS e roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante em vigência.

1.6.2. CONTROLE POR POLÍTICA DE FIREWALL

1.6.2.1. Suportar controle de políticas por porta e protocolo;

1.6.2.2. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento) e categorias de aplicações;

1.6.2.3. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.6.2.4. Controle, inspeção e de-criptografia SSL por política para tráfego de entrada (*inbound*) e saída (*outbound*);

1.6.2.5. Deve de-criptografar tráfego *inbound* e *outbound* em conexões negociadas com TLS 1.2;

1.6.2.6. É permitido o uso de *appliance* externo específico para a de-criptografia SSL e TLS com espelhamento do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise;

1.6.2.7. Bloqueio dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg;

1.6.2.8. QoS baseado em políticas (prioridade, garantia e máximo);

1.6.2.9. QoS baseado em políticas utilizando marcação de pacotes (*diffserv marking*), inclusive por aplicações;

1.6.2.10. Suportar objetos e regras IPv6;

1.6.2.11. Suportar objetos e regras *multicast*;

1.6.2.12. Suportar o agendamento das políticas com o objetivo de habilitar e desabilitá-las em horários pré-definidos;

1.6.3. CONTROLE DE APLICAÇÕES

1.6.3.1. Os *appliances* deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.6.3.1.1. Deve ser possível liberar e bloquear aplicações sem a necessidade de liberar portas e/ou protocolos;

1.6.3.1.2. Reconhecer, no mínimo, 1.500 (um mil e quinhentas) aplicações diferentes, incluindo, mas não limitado: tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, atualizações de software, protocolos de rede, VOIP, áudio, vídeo, proxies, mensageiros instantâneos, compartilhamento de arquivos e e-mail;

1.6.3.1.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

1.6.3.1.4. Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar através de expressões regulares e assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo. A inspeção deve determinar se uma aplicação está utilizando a porta padrão ou não, incluindo, mas não limitado a: RDP na porta 80 ao invés de 389;

1.6.3.1.5. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a: bittorrent criptografado e aplicações VOIP que utilizam criptografia proprietária;

1.6.3.1.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.

1.6.3.1.7. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante;

1.6.3.1.8. Deve realizar a decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do mesmo, validando se o tráfego corresponde à sua especificação, incluindo, mas não limitado a: Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a: compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

1.6.3.1.9. Identificar o uso de táticas evasivas via comunicações criptografadas;

1.6.3.1.10. Atualizar a base de assinaturas de aplicações automaticamente;

1.6.3.1.11. Reconhecer aplicações em IPv6;

1.6.3.1.12. Limitar a banda (*download* / *upload*) usada por aplicações utilizando QoS baseado no IP de origem, usuários e grupos do LDAP / AD;

1.6.3.1.13. Os *appliances* devem possuir a capacidade de identificar o usuário com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários;

1.6.3.1.14. Deve ser possível adicionar controle de aplicações através de regras de segurança do dispositivo;

1.6.3.1.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

1.6.3.1.16. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

1.6.3.1.17. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

1.6.3.1.18. Deve alertar o usuário quando uma aplicação for bloqueada;

1.6.3.1.19. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

1.6.3.1.20. Deve possibilitar a diferenciação de tráfego *peer-to-peer* (bittorrent, emule, neonet e etc.), *proxies* (ghostsurf, freegate, ultrasurf e etc.) e *Instant Messaging* (AIM, Gtalk, Facebook Chat, etc.), permitindo controle granular nas políticas definidas para ambos;

1.6.3.1.21. Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o Gtalk Chat e bloquear seu recurso de transferência de arquivos;

1.6.3.1.22. Deve ser possível a criação de grupos estáticos e dinâmicos de aplicações baseados em características das aplicações, tais como:

1.6.3.1.22.1. Tecnologia utilizada nas aplicações (cliente-servidor, baseado em navegador, protocolo de rede e etc.);

1.6.3.1.22.2. Nível de risco da aplicação;

1.6.3.1.22.3. Categoria e subcategoria de aplicações;

1.6.3.1.22.4. Aplicações que usem técnicas evasivas utilizadas por *malwares*, tais como: transferência de arquivos e/ou uso excessivo de banda;

1.6.4. PREVENÇÃO DE AMEAÇAS

1.6.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulos de IPS, *antivírus* e *anti-spyware* integrados no próprio *appliance* de firewall;

1.6.4.2. Deve incluir assinaturas de prevenção de IPS e bloqueio de arquivos maliciosos (*antivírus* e anti spyware);

1.6.4.3. As funcionalidades de IPS, *antivírus* e *anti-spyware* devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não

subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

1.6.4.4. Deve sincronizar as assinaturas de IPS, *antivírus*, anti spyware quando implementado em alta disponibilidade ativo/ativo ou ativo/passivo;

1.6.4.5. Quando utilizada as funções de IPS, *antivírus* e anti spyware, o *appliance* deve entregar a performance mínima estabelecida no edital entre ter uma única assinatura de IPS ou ter todas as assinaturas de IPS, *antivírus* e anti spyware habilitadas simultaneamente;

1.6.4.6. As assinaturas devem poder ser ativadas ou desativadas ou, ainda, habilitadas apenas em modo de monitoramento;

1.6.4.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

1.6.4.8. Deve suportar granularidade nas políticas de IPS, *antivírus* e anti spyware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.6.4.9. Deve permitir o bloqueio de vulnerabilidades;

1.6.4.10. Deve permitir o bloqueio de *exploits* conhecidos;

1.6.4.11. Deve incluir proteção contra ataques de negação de serviços;

1.6.4.12. Deverá possuir os seguintes mecanismos de inspeção de IPS:

1.6.4.12.1. Análise de padrões de estado de conexões;

1.6.4.12.2. Análise de decodificação de protocolo;

1.6.4.12.3. Análise para detecção de anomalias de protocolo;

1.6.4.12.4. Análise heurística;

1.6.4.12.5. IP *defragmentation*;

1.6.4.12.6. Bloqueio de pacotes malformados;

1.6.4.13. Ser imune e capaz de impedir ataques básicos, tais como: *syn flood*, *ICMP flood*, *UDP flood*;

1.6.4.14. Detectar e/ou bloquear a origem de um portscan;

1.6.4.15. Bloquear ataques efetuados por *worms* conhecidos;

1.6.4.16. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

1.6.4.17. Possuir assinaturas para bloqueio de ataques de *buffer overflow*;

1.6.4.18. Permitir o bloqueio de vírus e *spywares* em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP;

1.6.4.19. É permitido o uso de *appliance* externo (*antivírus* de rede), para o bloqueio de vírus e *spywares* em protocolo SMB de forma a conter *malwares* se espalhando horizontalmente pela rede;

1.6.4.20. Suportar bloqueio de arquivos por tipo;

1.6.4.21. Identificar e bloquear comunicação com *botnets*;

1.6.4.22. Deve suportar várias técnicas de prevenção, incluindo *drop* e/ou *tcp-rst*;

1.6.4.23. Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas:

1.6.4.23.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

1.6.4.24. Deve suportar a captura de pacotes (pcap), por assinatura de IPS e/ou *anti-spyware*;

1.6.4.25. Deve possuir a função de resolução de endereços DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo firewall com endereços (IPv4 e IPv6), previamente definidos;

1.6.4.26. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP;

1.6.4.27. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (*spyware*) e *worms*;

1.6.4.28. Proteção contra downloads de arquivos maliciosos involuntários usando HTTP;

1.6.4.29. Rastreamento de vírus em pdf;

1.6.4.30. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo *deflate* (zip, gzip, etc.);

1.6.4.31. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques, baseando-se em políticas de firewall que considere usuários, grupos de usuários, origem e destino;

1.6.5. ANÁLISE DE MALWARES MODERNOS

1.6.5.1. Possuir a capacidade de análise de ameaças não conhecidas;

1.6.5.2. A solução ofertada dever possuir funcionalidades para análise de *malwares* não conhecidos incluídas na própria ferramenta ou entregue em composição com outro fabricante;

1.6.5.3. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "in cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

1.6.5.4. Selecionar através de política de firewall quais tipos de arquivos sofrerão esta análise;

1.6.5.5. A análise deverá considerar, pelo menos, 100 (cem) tipos de comportamentos maliciosos distintos para determinar se o arquivo é malicioso ou não;

1.6.5.6. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistemas operacionais Windows XP e Windows 7;

1.6.5.7. Deve suportar o monitoramento de arquivos trafegados na internet (HTTP, FTP, HTTP, SMTP) como também arquivos trafegados internamente nos servidores de arquivos usando SMB;

1.6.5.8. O sistema de análise "in cloud" ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar ou propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de *antivírus* e *anti-spyware* automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede);

1.6.5.9. O sistema automático de analise "in cloud" ou local deve emitir relatório com identificação de quais soluções de *antivírus* existentes no mercado possuem assinaturas para bloquear o malware;

1.6.5.10. Deve permitir exportar o resultado das análises de *malwares* de dia zero em PDF e CSV a partir da própria interface de gerência;

1.6.5.11. Deve permitir o download dos *malwares* identificados a partir da própria interface de gerência;

1.6.5.12. Deve permitir visualizar os resultados das análises de *malwares* de dia zero nos diferentes sistemas operacionais suportados;

1.6.5.13. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de *malwares* de dia zero a partir da própria interface de gerência;

1.6.5.14. Suportar a análise de arquivos executáveis, dll, ZIP e criptografados em SSL no ambiente controlado.

1.6.6. FILTRO DE URL

1.6.6.1. Apenas os equipamentos do site principal precisam conter filtro de URL, tendo conformidade com os seguintes requisitos:

1.6.6.1.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.6.6.1.2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IP e redes;

1.6.6.1.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-Directory e base de dados local;

1.6.6.1.4. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

1.6.6.1.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

1.6.6.1.6. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção *Safe Search* esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

1.6.6.1.7. Suporta base ou cache de URLs local no *appliance*, evitando *delay* de comunicação ou validação das URLs;

1.6.6.1.8. Possuir pelo menos 60 categorias de URLs;

1.6.6.1.9. Suportar a criação de categorias de URL customizadas;

1.6.6.1.10. Suportar a exclusão de URL do bloqueio, por categoria;

1.6.6.1.11. Permitir a customização de página de bloqueio;

1.6.6.1.12. Permitir o bloqueio e continuação (o usuário é bloqueado, mas pode avançar na navegação ao clicar em uma opção "continuar");

1.6.6.1.13. Suportar a inclusão nos logs do produto de informações das atividades dos usuários.

1.6.7. IDENTIFICAÇÃO DE USUÁRIOS

1.6.7.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-Directory e base de dados local;

1.6.7.2. Deve possuir integração com Microsoft Active Directory, RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle baseada em usuários e grupos de usuários;

1.6.7.3. Deve permitir o controle, sem instalação de software cliente, em equipamentos que solicitem saída à internet, para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (*Captive Portal*);

1.6.7.4. Suporte a autenticação Kerberos;

1.6.7.5. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

1.6.7.6. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows;

1.6.8. QoS

1.6.8.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo (youtube, ustream e etc.) e ter um alto consumo de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, tenha a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo *streaming*;

1.6.8.2. Suportar a criação de políticas de QoS por:

1.6.8.2.1. Endereço de origem;

1.6.8.2.2. Endereço de destino;

1.6.8.2.3. Por usuário e grupo do LDAP/AD;

1.6.8.2.4. Por aplicações, incluindo, mas não limitado a: Skype, Bittorrent, YouTube e Azureus;

1.6.8.2.5. Por porta;

1.6.8.3. O QoS deve possibilitar a definição de classes por:

1.6.8.3.1. Banda garantida;

1.6.8.3.2. Banda máxima;

1.6.8.3.3. Fila de prioridade;

1.6.8.4. Suportar priorização de tempo real de protocolos de voz (VOIP), tais como: H.323, SIP, SCCP, MGCP e aplicações como Skype;

1.6.8.5. Suportar marcação de pacotes *Diffserv*, inclusive por aplicação;

1.6.8.6. Disponibilizar estatísticas de tempo real para classes de QoS;

1.6.8.7. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e usuário.

1.6.9. FILTRO DE DADOS

1.6.9.1. Permitir a criação de filtros para arquivos e dados pré-definidos;

1.6.9.2. Os arquivos devem ser identificados por extensão e assinaturas;

1.6.9.3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, dentre outros) identificados sobre aplicações (P2P, *Instant Messaging*, SMB, dentre outros);

1.6.9.4. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.6.9.5. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a: número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

1.6.9.6. Permitir listar o número de aplicações suportadas para controle de dados;

1.6.9.7. Permitir listar o número de tipos de arquivos suportados para controle de dados.

1.6.10. GEOLOCALIZAÇÃO

1.6.10.1. Suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinados países seja bloqueado;

1.6.10.2. Deve possibilitar a visualização dos países de origem e destino nos logs;

1.6.10.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica, tornando possível sua utilização em políticas de firewall.

1.6.11. VPN

1.6.11.1. Suportar VPN *site-to-site* e cliente-to-site;

1.6.11.2. Suportar IPSec VPN;

1.6.11.3. Suportar SSL VPN;

1.6.11.4. A VPN IPSec deve suportar:

1.6.11.4.1. 3DES;

1.6.11.4.2. Autenticação MD5 e SHA-1;

1.6.11.4.3. Diffie-Hellman group 1, group 2, group 5 e group 14;

1.6.11.4.4. Algoritmo *Internet Key Exchange* (IKE);

1.6.11.4.5. AES (*Advanced Encryption Standard*); 128 e 256;

1.6.11.4.6. Autenticação via certificado IKE PKI;

1.6.11.5. Deve possuir interoperabilidade com os seguintes fabricantes:

1.6.11.5.1. Cisco;

1.6.11.5.2. Checkpoint;

1.6.11.5.3. Juniper;

1.6.11.5.4. Palo Alto Networks;

1.6.11.5.5. Fortinet;

1.6.11.5.6. Sonic Wall;

1.6.11.6. A VPN SSL deve suportar:

1.6.11.6.1.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface Web;

1.6.11.6.1.2. A funcionalidade de VPN SSL deve ser atendida com ou sem o uso de agente;

1.6.11.6.1.3. Atribuição de endereço IP nos clientes remotos de VPN;

1.6.11.6.1.4. Atribuição de DNS nos clientes remotos de VPN;

1.6.11.6.1.5. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;

1.6.11.6.1.6. Deve permitir criar políticas de controle de aplicações, IPS, *antivírus*, *anti-spyware* e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

1.6.11.6.1.7. A VPN SSL deve suportar proxy ARP e uso de interfaces PPPoE;

1.6.11.6.1.8. Suportar autenticação via AD/LDAP, Secure ID, certificado e base local de usuários;

1.6.11.6.1.9. Permitir estabelecer um túnel VPN *client-to-site* do cliente à plataforma de segurança, fornecendo uma solução de *single-sign-on* aos usuários, integrando-se com as ferramentas de Windows-logon;

1.6.11.6.1.10. Suportar a leitura e verificação de CRL (*Certificate Revocation List*);

1.6.11.6.1.11. Permitir a aplicação de políticas de segurança e dispor de visibilidade para as aplicações que circulam dentro dos túneis SSL;

1.6.11.6.1.12. O agente de VPN a ser instalado nos equipamentos desktop e laptops deve ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

1.6.11.6.1.13. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;

1.6.11.7. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

1.6.11.7.1.1. Antes do usuário autenticar na estação;

1.6.11.7.1.2. Após autenticação do usuário na estação;

1.6.11.7.1.3. Sob demanda do usuário;

1.6.11.8. Deverá manter uma conexão segura com o portal durante a sessão;

1.6.11.9. O agente de VPN SSL *client-to-site* deve ser compatível com pelo menos os seguintes sistemas operacionais: Windows XP, Windows Vista, Windows 7, Windows 8 e Mac OSx;

1.6.12. SISTEMA DE GERÊNCIA E MONITORAÇÃO CENTRALIZADA

1.6.12.1. Centralizar a administração de regras e políticas dos equipamentos fornecidos, usando uma única interface de gerenciamento;

1.6.12.2. Será permitido o fornecimento desta solução de gerência e monitoramento centralizado como *appliances* virtual, o mesmo deverá ser compatível com VMWare ESXi 4.0, ou superior;

1.6.12.3. O gerenciamento da solução deve suportar acesso via SSH, cliente remoto e/ou web por HTTPS;

1.6.12.4. Caso haja a necessidade de instalação de cliente para administração da solução, o mesmo deve ser compatível com sistemas operacionais Windows;

1.6.12.5. O gerenciamento deve permitir ou possuir:

1.6.12.5.1. Criação e administração de políticas de firewall e controle de aplicação;

1.6.12.5.2. Criação e administração de políticas de IPS, *antivírus* e *anti-spyware*;

1.6.12.5.3. Criação e administração de políticas de filtro de URL;

1.6.12.5.4. Monitoramento de logs;

1.6.12.5.5. Ferramentas de investigação de logs;

1.6.12.5.6. Recursos para troubleshooting;

1.6.12.5.7. Captura de pacotes;

1.6.12.5.8. Acesso concorrente de administradores;

1.6.12.5.9. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

1.6.12.5.10. Deve permitir usar palavras-chave e cores para facilitar a identificação de regras;

1.6.12.5.11. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes de alimentação, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site e número de sessões estabelecidas;

1.6.12.5.12. Bloqueio de "*commit*" das configurações do firewall, no caso de acesso simultâneo de dois ou mais administradores;

1.6.12.5.13. Definição de perfis de acesso na console com permissões granulares, tais como: acesso de escrita, acesso de leitura, criação de usuários e alteração de configurações;

1.6.12.5.14. Autenticação integrada ao Microsoft Active Directory e servidor RADIUS;

1.6.12.5.15. Localização de em quais regras um endereço IP, IP range, subnet ou objetos estão sendo utilizados;

1.6.12.5.16. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QoS e regras de DOS;

1.6.12.5.17. Criação de regras que fiquem ativas em horário definido;

1.6.12.5.18. Criação de regras com data de expiração;

1.6.12.5.19. Backup das configurações e rollback de configuração para a última configuração salva;

1.6.12.5.20. Suportar rollback de sistema operacional para a última versão local;

1.6.12.5.21. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

1.6.12.5.22. Validação de regras antes da aplicação;

1.6.12.5.23. É permitido o uso de *appliance* externo para realizar a validação de regras antes da aplicação;

1.6.12.5.24. Validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing). É permitida a utilização de *appliance* externo;

1.6.12.5.25. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

1.6.12.5.26. Deve possibilitar a integração com soluções de SIEM de mercado;

1.6.12.5.27. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

1.6.12.5.28. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, permitindo a comparação dos diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

1.6.12.5.29. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado;

1.6.12.6. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, *antivírus* e *anti-spyware*), URL e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

1.6.12.7. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelo dispositivo de segurança;

1.6.12.8. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, *antivírus* e anti-spware) e etc.;

1.6.12.9. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, *antivírus* e anti-spware) e URLs que passaram pela solução;

1.6.12.10. Deve possuir mecanismo "*drill-down*" para navegação nos relatórios em tempo real;

1.6.12.11. Nas opções de "*drill-down*", ser possível identificar o usuário que fez determinado acesso;

1.6.12.12. Deve ser possível exportar os logs em CSV;

1.6.12.13. Deverá ser possível acessar a gerencia para visualizar ou aplicar configurações durante os momentos onde o trafego é muito alto e a CPU e memória do equipamento estiverem com taxas maiores que 99% de utilização;

1.6.12.14. Rotação do log;

1.6.12.15. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

1.6.12.15.1. Situação do dispositivo e do cluster;

1.6.12.15.2. Principais aplicações;

1.6.12.15.3. Principais aplicações por risco;

1.6.12.15.4. Administradores autenticados na gerência da plataforma de segurança;

1.6.12.15.5. Número de sessões simultâneas;

1.6.12.15.6. Status das interfaces;

1.6.12.15.7. Uso de CPU;

1.6.12.16. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

1.6.12.16.1. Resumo gráfico de aplicações utilizadas;

1.6.12.16.2. Principais aplicações por utilização de largura de banda de entrada e saída;

1.6.12.16.3. Principais aplicações por taxa de transferência de bytes;

1.6.12.16.4. Principais hosts por número de ameaças identificadas;

1.6.12.16.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL e tempo de utilização e ameaças (IPS, *antivírus* e anti-spware) vinculadas a este tráfego;

1.6.12.16.6. Deve permitir a criação de relatórios personalizados;

1.6.12.17. Em cada critério de pesquisa do log, deve ser possível incluir múltiplas entradas (por exemplo, 10 redes e IPs distintos, serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

1.6.12.18. Gerar alertas automáticos via:

1.6.12.18.1. E-mail;

1.6.12.18.2. SNMP;

1.6.12.18.3. Syslog;

1.7. CARACTERÍSTICAS ESPECÍFICAS PARA OS 2 (DOIS) EQUIPAMENTOS STANDALONE QUE CONECTARÃO OS ESCRITÓRIOS REMOTOS:

1.7.1. CAPACIDADE E QUANTIDADE

1.7.1.1. *Throughput* mínimo de 100 Mbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

1.7.1.2. Os appliances ofertados deverão possuir em validade a certificação *Common Criteria EAL-4* ou ICSA Labs (firewall);

1.7.1.3. Suporte a, no mínimo, 64.000 conexões simultâneas;

1.7.1.4. Suporte a, no mínimo, 1.000 novas conexões por segundo;

1.7.1.5. Fonte de alimentação 100/240VAC;

1.7.1.6. 4 (quatro) interfaces de rede 10/100/1000 base-tx;

1.7.1.7. Deve possuir uma interface de rede dedicada para gerenciamento;

1.7.1.8. Deve possuir uma interface do tipo console ou similar;

1.7.1.9. Estar licenciada para suportar sem o uso de licença 25 (vinte e cinco) túneis de VPN IPSec simultâneos;

1.7.1.10. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

1.7.1.11. Por console de gerência e monitoramento, entende-se as licenças de software necessárias para as duas funcionalidades;

1.7.1.12. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de *end-of-life* e *end-of-sale*.

1.7.2. CARACTERÍSTICAS GERAIS

1.7.2.1. A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência e monitoramento;

1.7.2.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

1.7.2.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliance*s, desde que obedeçam a todos os requisitos desta especificação;

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

1.7.2.5. O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoramento, devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.7.2.6. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.7.2.6.1. Suporte a 1024 VLAN *tags* 802.1q;

1.7.2.6.2. Suporte a PBR (*Policy Based Routing*) ou PBF (*Policy Based Forwarding*);

1.7.2.6.3. Roteamento *multicast* (PIM-SM);

1.7.2.6.4. DHCP *relay*;

1.7.2.6.5. DHCP *server*;

1.7.2.6.6. Suporte à criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

1.7.2.7. Suportar subinterfaces ethernet lógicas.

1.7.2.8. Deve suportar os seguintes tipos de NAT:

1.7.2.8.1. Nat dinâmico (n:1);

1.7.2.8.2. Nat dinâmico (n:n);

1.7.2.8.3. Nat estático (1:1);

1.7.2.8.4. NAT estático (n:n);

1.7.2.8.5. Nat estático bidirecional (1:1);

1.7.2.8.6. Tradução de porta (PAT);

1.7.2.8.7. NAT de origem;

1.7.2.8.8. NAT de destino;

1.7.2.8.9. Suportar NAT de origem e NAT de destino simultaneamente;

1.7.2.9. Enviar log para um ou mais sistemas de monitoramento de maneira simultânea;

1.7.2.10. Deve haver a opção de enviar logs para os sistemas de monitoramento externos via protocolo TCP e SSL;

1.7.2.11. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoramento externo de logs;

1.7.2.12. Proteção contra *anti-spoofing*;

1.7.2.13. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

1.7.2.14. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

1.7.2.15. Suportar a OSPF *graceful restart*;

1.7.2.16. Suportar, no mínimo, as seguintes funcionalidades em IPv6: SLAAC (*Address Auto Configuration*), NAT64, identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, regras de proteção contra DoS (*Denial of Service*), de-criptografia SSL, PBF (*Policy Based Forwarding*), QoS, DHCPv6 *relay*, SNMP, NTP, SYSLOG, DNS e controle de aplicação;

1.7.2.17. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos: modo *sniffer* (monitoramento e análise do tráfego), camada 2 (L2) e camada 3 (L3);

1.7.2.18. Modo *sniffer*, para inspeção via porta espelhada;

1.7.2.19. Modo L2, para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

1.7.2.20. Modo L3, para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação, operando como *default gateway* das redes protegidas;

1.7.2.21. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QoS, SSL *decryption* e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo

ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

1.7.3. CONTROLE POR POLÍTICA DE FIREWALL

1.7.3.1. Controles de políticas por porta e protocolo;

1.7.3.2. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

1.7.3.3. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.7.3.4. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (*inbound*) e saída (*outbound*).

1.7.3.5. Deve de-criptografar tráfego *inbound* e *outbound* em conexões negociadas com TLS 1.2;

1.7.3.6. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;

1.7.3.7. QoS baseado em políticas (prioridade, garantia e máximo);

1.7.3.8. QoS baseado em políticas para marcação de pacotes (*diffserv marking*), inclusive por aplicações;

1.7.3.9. Suporte a objetos e regras IPv6;

1.7.3.10. Suporte a objetos e regras *multicast*;

1.7.3.11. Suportar o agendamento de políticas para que sejam habilitadas ou desabilitadas conforme horário pré-definido;

1.7.4. CONTROLE DE APLICAÇÕES

1.7.4.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.7.4.1.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

1.7.4.1.2. Reconhecer pelo menos 1.500 aplicações diferentes, incluindo, mas não limitado: tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.7.4.1.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

1.7.4.1.4. Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta *default* ou não, incluindo, mas não limitado a: RDP na porta 80 ao invés de 389;

1.7.4.1.5. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado;

1.7.4.1.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que se utilizam de táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;

1.7.4.1.7. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante;

1.7.4.1.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do mesmo, validando se o tráfego atende às suas especificações, incluindo, mas não limitado a: Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a: compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

1.7.4.1.9. Identificar o uso de táticas evasivas via comunicações criptografadas;

1.7.4.1.10. Atualizar a base de assinaturas de aplicações automaticamente;

1.7.4.1.11. Reconhecer aplicações em IPv6;

1.7.4.1.12. Limitar a banda (download/upload) usada por aplicações (*traffic shaping*), baseando-se no IP de origem, usuários e grupos do LDAP/AD;

1.7.4.1.13. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários;

1.7.4.1.14. Deve ser possível adicionar controle de aplicações nas regras de segurança do dispositivo;

1.7.4.1.15. Deve entregar métodos de identificação e classificação das aplicações;

1.7.4.1.16. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

1.7.4.1.17. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

1.7.4.1.18. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

1.7.4.1.19. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;

1.7.4.1.20. Deve possibilitar a diferenciação de aplicações *proxies* (ghostsurf, freegate, dentre outros), *Instant Messaging* (AIM, Gtalk, Facebook Chat, dentre outros), *peer-to-peer* (Bittorrent, emule, neonet, dentre outros) permitindo um controle granular na configuração de políticas;

1.7.4.1.21. Deve ser possível a criação de grupos estáticos e dinâmicos de aplicações, baseando-se em suas características, tais como:

1.7.4.1.21.1. Tecnologia utilizada nas aplicações (*client-server*, *browser based*, *Network Protocol* e etc.);

1.7.4.1.21.2. Nível de risco da aplicação;

1.7.4.1.21.3. Categoria e subcategoria de aplicações;

1.7.4.1.21.4. Aplicações que usem técnicas evasivas, utilizadas por *malwares*, como transferência de arquivos e/ou uso excessivo de banda.

1.7.5. VPN

1.7.5.1. Suportar VPN *site-to-site* e *client-to-site*;

1.7.5.2. Suportar IPSec VPN;

1.7.5.3. Suportar SSL VPN;

1.7.5.4. A VPN IPSec deve suportar:

1.7.5.4.1. 3DES;

1.7.5.4.2. Autenticação MD5 e SHA1;

1.7.5.4.3. *Diffie-Hellman* grupo 1, grupo 2, grupo 5 e grupo 14;

1.7.5.4.4. Algoritmo *Internet Key Exchange* (IKE);

1.7.5.4.5. AES 128 e 256 (Advanced Encryption Standard);

1.7.5.4.6. Autenticação via certificado IKE PKI;

1.7.5.5. Deve possuir interoperabilidade com os seguintes fabricantes:

1.7.5.5.1. Cisco;

1.7.5.5.2. Checkpoint;

1.7.5.5.3. Juniper;

1.7.5.5.4. Palo Alto Networks;

1.7.5.5.5. Fortinet;

1.7.5.5.6. Sonic Wall;

1.7.5.6. A VPN SSL deve suportar:

1.7.5.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface *web*;

1.7.5.6.2. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

1.7.5.6.3. Atribuição de endereço IP nos clientes remotos de VPN;

1.7.5.6.4. Atribuição de DNS nos clientes remotos de VPN;

1.7.5.6.5. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;

1.7.5.6.6. Dever permitir criar políticas de controle de aplicações, IPS, *antivírus*, *anti-spyware* e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

1.7.5.6.7. A VPN SSL deve suportar proxy ARP e uso de interfaces PPPoE;

1.7.5.6.8. Suportar autenticação via AD/LDAP, *Secure ID*, certificado e base de usuários local;

1.7.5.6.9. Permitir que se estabeleça um túnel VPN *client-to-site* do cliente com a plataforma de segurança, fornecendo uma solução de *single-sign-on* aos usuários, integrando-se com as ferramentas de Windows-Logon;

1.7.5.6.10. Suporta leitura e verificação de CRL (*Certificate Revocation List*);

1.7.5.6.11. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

1.7.5.6.12. O agente de VPN a ser instalado nos equipamentos desktop e laptops, deve ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

1.7.5.6.13. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;

1.7.5.6.14. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

1.7.5.6.14.1. Antes do usuário autenticar na estação;

1.7.5.6.14.2. Após autenticação do usuário na estação;

1.7.5.6.14.3. Sob demanda do usuário;

1.7.5.6.15. Deverá manter uma conexão segura com o portal durante a sessão;

1.7.5.6.16. O agente de VPN SSL *client-to-site* deve ser compatível, pelo menos, os seguintes sistemas operacionais: Windows XP, Windows Vista, Windows 7, Windows 8 e Mac OSx;

1.7.6. SISTEMA DE GERÊNCIA E MONITORAÇÃO CENTRALIZADO

1.7.6.1. O gerenciamento da solução deve suportar acesso via SSH, cliente remoto e/ou web por HTTPS;

1.7.6.2. Caso haja a necessidade de instalação de cliente para administração da solução, o mesmo deve ser compatível com sistemas operacionais Windows;

1.7.6.3. O gerenciamento deve permitir ou possuir:

1.7.6.3.1. Criação e administração de políticas de firewall e controle de aplicação;

1.7.6.3.2. Criação e administração de políticas de IPS, *antivírus* e *anti-spyware*;

1.7.6.3.3. Criação e administração de políticas de filtro de URL;

1.7.6.3.4. Monitoramento de logs;

1.7.6.3.5. Ferramentas de investigação de logs;

1.7.6.3.6. Recursos para troubleshooting;

1.7.6.3.7. Captura de pacotes;

1.7.6.3.8. Acesso concorrente de administradores;

1.7.6.3.9. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

1.7.6.3.10. Deve permitir usar palavras-chave e cores para facilitar a identificação de regras;

1.7.6.3.11. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes de alimentação, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site e número de sessões estabelecidas;

1.7.6.3.12. Bloqueio de "*commit*" das configurações do firewall, no caso de acesso simultâneo de dois ou mais administradores;

1.7.6.3.13. Definição de perfis de acesso na console com permissões granulares, tais como: acesso de escrita, acesso de leitura, criação de usuários e alteração de configurações;

1.7.6.3.14. Autenticação integrada ao Microsoft Active Directory e servidor RADIUS;

1.7.6.3.15. Localização de em quais regras um endereço IP, IP range, subnet ou objetos estão sendo utilizados;

1.7.6.3.16. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QoS e regras de DOS;

1.7.6.3.17. Criação de regras que fiquem ativas em horário definido;

1.7.6.3.18. Criação de regras com data de expiração;

1.7.6.3.19. Backup das configurações e rollback de configuração para a última configuração salva;

1.7.6.3.20. Suportar rollback de sistema operacional para a última versão local;

1.7.6.3.21. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

1.7.6.3.22. Validação de regras antes da aplicação;

1.7.6.4. É permitido o uso de *appliance* externo para realizar a validação de regras antes da aplicação;

1.7.6.5. Validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (*shadowing*). É permitida a utilização de *appliance* externo;

1.7.6.6. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

1.7.6.7. Deve possibilitar a integração com soluções de SIEM de mercado;

1.7.6.8. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

1.7.6.9. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, permitindo a comparação dos diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

1.7.6.10. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado;

1.7.6.11. Deve prover relatórios com visão correlacionada de aplicações, e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

1.7.6.12. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelo dispositivo de segurança;

1.7.6.13. Deve possuir relatórios de utilização dos recursos por aplicações, filtro de arquivos, etc.;

1.7.6.14. Prover uma visualização sumarizada de todas as aplicações, que passaram pela solução;

1.7.6.15. Deve possuir mecanismo "*drill-down*" para navegação nos relatórios em tempo real;

1.7.6.16. Nas opções de "*drill-down*", ser possível identificar o usuário que fez determinado acesso;

1.7.6.17. Deve ser possível exportar os logs em CSV;

1.7.6.18. Deverá ser possível gerenciar os equipamentos, tanto para visualizar como aplicar configurações, durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiverem com taxas maiores que 99% de utilização;

1.7.6.19. Rotação do log;

1.7.6.20. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

1.7.6.20.1. Situação do dispositivo e do cluster;

1.7.6.20.2. Principais aplicações;

1.7.6.20.3. Principais aplicações por risco;

1.7.6.20.4. Administradores autenticados na gerência da plataforma de segurança;

1.7.6.20.5. Número de sessões simultâneas;

1.7.6.20.6. Status das interfaces;

1.7.6.20.7. Uso de CPU;

1.7.6.21. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

1.7.6.21.1. Resumo gráfico de aplicações utilizadas;

1.7.6.21.2. Principais aplicações por utilização de largura de banda de entrada e saída;

1.7.6.21.3. Principais aplicações por taxa de transferência de bytes;

1.7.6.21.4. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas;

1.7.6.21.5. Deve permitir a criação de relatórios personalizados;

1.7.6.22. Em cada critério de pesquisa do log, deve ser possível incluir múltiplas entradas (por exemplo, 10 redes e IPs distintos, serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

1.7.6.23. Gerar alertas automáticos via:

1.7.6.23.1. E-mail;

1.7.6.23.2. SNMP;

1.7.6.23.3. Syslog;

ANEXO II

ESTIMATIVA DE CUSTOS

VALORES MÁXIMOS QUE A ADMINISTRAÇÃO SE PROPÕE A PAGAR

SOLUÇÃO PARA FIREWALL						
ITEM	**SUBITEM**	**BEM / SERVIÇO**	**QTDE**	**Un.**	**VALOR UNITÁRIO - R$**	**VALOR TOTAL - R$**
1	**1.1**	Firewall Appliance Tipo 1	**2**	**Solução**	**R$ 314.915,49**	**R$ 629.830,99**
	1.2	Firewall Appliance Tipo 2	**2**	**Solução**	**R$ 226.668,74**	**R$ 453.337,48**
	1.3	Firewall Appliance Tipo 3	**2**	**Solução**	**R$ 45.593,08**	**R$ 91.186,17**
	1.4	Gerência e Monitoração Centralizada	**1**	**Sistema**	**R$ 85.555,62**	**R$ 85.555,62**
	1.5	Instalação e Configuração	**1**	**Serviço**	**R$ 71.626,15**	**R$ 71.626,15**
	1.6	Transferência de Conhecimento	**1**	**Turma**	**R$ 30.327,47**	**R$ 30.327,47**
	1.7	Suporte Técnico	**48**	**Meses**	**R$ 2.673,73**	**R$ 128.338,88**
TOTAL						**R$ 1.490.202,76**

ANEXO III

MODELO DE PROPOSTA

IDENTIFICAÇÃO DA EMPRESA:
Razão social e CNPJ:
Responsável para contato:
Endereço:
Telefone/Fax/E-mail:

1. À
PROCURADORIA-GERAL DO DISTRITO FEDERAL
Setor de Administração Municipal – SAM – Projeção "I", Asa Norte, Brasília – DF.

Proposta que faz a (razão social da licitante)_____ inscrita no CNPJ nº _____, solução de segurança de rede, composta por 6 (seis) firewalls *appliances*, sistema de gerência e monitoração centralizada, serviços de instalação e configuração, transferência de conhecimento e suporte técnico on-site em garantia, a fim de atender as necessidades corporativas da Casa, conforme produtos, especificações e condições constantes do Termo de Referência e Anexo I.1, do edital.

2. PREÇOS:

SOLUÇÃO PARA FIREWALL						
ITEM	**BITEM**	**BEM / SERVIÇO**	**QTDE**	**Un.**	**VALOR UNITÁRIO - R$**	**VALOR TOTAL - R$**
1	**1.1**	Firewall Appliance Tipo 1	**2**	**Solução**		
	1.2	Firewall Appliance Tipo 2	**2**	**Solução**		
	1.3	Firewall Appliance Tipo 3	**2**	**Solução**		
	1.4	Gerência e Monitoração Centralizada	**1**	**Sistema**		
	1.5	Instalação e Configuração	**1**	**Serviço**		
	1.6	Transferência de Conhecimento	**1**	**Turma**		
	1.7	Suporte Técnico	**48**	**Meses**		

Valor total da proposta (por extenso):

3. ENTREGA E GARANTIA
Prazos de entrega Conforme estabelecido no tópico 6.5.1 do Termo de Referência.

4. Período de garantia: Conforme estabelecido no tópico 5.5 do Termo de Referência.

5. VALIDADE DA PROPOSTA
Prazo de validade: _____(não inferior a 60 (sessenta) dias corridos), a contar da data da licitação.

6. COMPOSIÇÃO DOS PREÇOS

Nos preços propostos acima estão incluídas todas as despesas, frete, tributos e demais encargos de qualquer natureza incidentes sobre o objeto deste Pregão.

7. DECLARAÇÕES

Esta licitante declara que atenderá integralmente para a execução do contrato as especificações, condições e prazos estabelecidos no Edital e seus Anexos.

Segue em anexo, **toda documentação necessária** para subsidiar o julgamento técnico da solução ofertada quanto ao atendimento das funcionalidades descritas no Termo de Referência, Anexo I e I.1 do Edital.

(Local e data)

Assinatura do Representante Legal
da Licitante

(Contendo a identificação com NOME COMPLETO)

ANEXO IV

MODELO DE COMPROVAÇÃO PONTUAL DE ATENDIMENTO À ESPECIFICAÇÃO TÉCNICA

1. Modelo de comprovação pontual de atendimento à Especificação Técnica:

TÓPICO	DESCRIÇÃO	PROPOSTA ATENDE?	REFERÊNCIA NA DOCUMENTAÇÃO TÉCNICA	OBSERVAÇÃO
1.6.1.3	Os *appliances* ofertados deverão possuir em validade a certificação *Common Criteria* EAL-4 ou ICSA *Labs* (firewall);	SIM	Manual xxx, Pag. 23, Paragrafo 12; Manual zzz, Pag. 03, Linha 2;	
1.6.1.9	*Possuir 1 (uma) interface ethernet dedicada para gerenciamento e monitoramento;*	SIM	Datasheet yyy, Pag. 11 e 12;	

Local e data
Assinatura e carimbo
(Representante Legal)

Observação: Emitir em papel que identifique o **Licitante.**

Brasília, _____ de _____ de 20____

ANEXO V-A

MODELO DE DECLARACAO DE VISTORIA TÉCNICA

Pelo presente, declaramos para fins de participação do processo licitatório para aquisição de *Firewall*s (conforme Termo de Referência e seus anexos), que o(a) Sr.(a) _____, representante da empresa _____, CNPJ nº _____, situada no endereço_____ compareceu a Procuradoria-Geral do Distrito Federal, **para se cientificar das peculiaridades**, dos atuais equipamentos de rede e segurança, das condições no local, do ambiente, das possíveis dificuldades, do padrão das instalações, configurações e da forma das substituições dos equipamentos de rede da Procuradoria Geral do DF a serem executadas, assumindo total responsabilidade pelo cumprimento das substituições, instalações e configurações dos aparelhos adquiridos e garantia do perfeito funcionamento dos *Firewall*s na rede da PGDF.

_____, _____, de _____ de 2015.

_____

Carimbo e assinatura do representante legal da empresa

Nome:_____

Cargo:_____

RG:_____

OBS: Esta declaração deverá ser entregue junto com a documentação de HABILITAÇÃO

ANEXO V-B

MODELO DE DECLARACAO DE DESISTÊNCIA DE VISTORIA TÉCNICA

Pelo presente, a empresa _____,

CNPJ nº _____, situada no endereço: _____, por intermédio de seu Representante Legal, o(a) Sr. (a) _____, apresenta **DESISTÊNCIA FORMAL DE VISITA TÉCNICA**, para fins de participação do processo licitatório para aquisição de *Firewall*s (conforme Termo de Referência e seus anexos), **abdicando do direito de se cientificar das peculiaridades,** dos atuais equipamentos de rede e segurança, das condições no local, do ambiente, das possíveis dificuldades, do padrão das instalações, configurações e da forma das substituições dos equipamentos de rede da Procuradoria Geral do DF a serem executadas, assumindo total responsabilidade pelo cumprimento das substituições, instalações e configurações dos aparelhos adquiridos e garantia do perfeito funcionamento dos *Firewall*s na rede da PGDF, pelo valor global da proposta.

_____, _____, de _____ de 2015.

_____

Carimbo e assinatura do representante legal da empresa

Nome:_____

Cargo:_____

RG:_____

OBS: Esta declaração deverá ser entregue junto com a documentação de HABILITAÇÃO.

ANEXO VI

MODELO

DECLARAÇÃO
DE QUE NÃO EMPREGA MENOR

A empresa _____, inscrita no CNPJ sob o nº _____, sediada no endereço _____, telefone/fax nº _____, por intermédio do seu representante legal Sr(a). _____ _____, portador(a) da Carteira de Identidade nº _____ e do CPF nº _____, DECLARA para fins do disposto no inciso V do art. 27 da Lei Federal nº. 8.666, de 21 de junho de 1993, acrescido pela Lei nº. 9.854, de 27 de outubro de 1999, em conformidade com o previsto no inciso XXXIII, do art. 7º, da Constituição Federal/88, que não possui em seu quadro de pessoal empregado(s) menor (es) de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos 14 (quatorze) anos.

_____
Local e Data

_____
[Nome do Representante Legal da Empresa]
Cargo

ANEXO VII

MODELO DE TERMO DE CONFIDENCIALIDADE

0. INTRODUÇÃO:

A **<PESSOA JURÍDICA OU FÍSICA CONTRATADA>**, doravante referida simplesmente como CONTRATADA, inscrita no CNPJ/MF sob o número <NÚMERO DO CNPJ>, com endereço <ENDEREÇO>, neste ato representado pelo <VÍNCULO DO SIGNATÁRIO COM A CONTRATADA>, **<NOME DO SIGNATÁRIO>**, nos termos do <CONTRATO OU TERMO ADITIVO EM QUE FOI PACTUADO O SIGILO>, compromete-se a observar o presente TERMO DE CONFIDENCIALIDADE, firmado perante o **DISTRITO FEDERAL**, por meio da **PROCURADORIA GERAL DO DISTRITO FEDERAL**, doravante referida simplesmente como **PGDF**, em conformidade com as cláusulas que seguem:

1. CLÁUSULA PRIMEIRA – DO OBJETO:
O objeto deste TERMO DE CONFIDENCIALIDADE é a necessária e adequada proteção às informações confidenciais fornecidas à CONTRATADA para que possa desenvolver as atividades contempladas especificamente no Contrato nº ____/_____.

Subcláusula Primeira - As estipulações constantes neste TERMO DE CONFIDENCIALIDADE se aplicam a toda e qualquer informação revelada à CONTRATADA.

Subcláusula Segunda - A CONTRATADA reconhece que, em razão da prestação de serviços à PGDF, tem acesso a informações que pertencem à PGDF, que devem ser tratadas como sigilosas.

2. CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS
Deve ser considerada confidencial toda e qualquer informação observada ou revelada, por qualquer meio, em decorrência da execução do contrato, contendo ela ou não a expressão “CONFIDENCIAL”.
Subcláusula Primeira - O termo “Informação” abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: diagramas de redes, fluxogramas, processos, projetos, ambiente físico e lógico, topologia de redes, configurações de equipamentos, entre outras a que, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, venha a CONTRATADA ter acesso durante ou em razão da execução do contrato celebrado.

Subcláusula Segunda - Em caso de dúvida acerca da natureza confidencial de determinada informação, a CONTRATADA deverá mantê-la sob sigilo até que seja autorizada expressamente pelo representante legal da PGDF, referido no Contrato, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa da PGDF poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

3. CLÁUSULA TERCEIRA - DOS LIMITES DA CONFIDENCIALIDADE
As estipulações e obrigações constantes do presente instrumento não serão aplicadas a nenhuma informação que:
I - seja comprovadamente de conhecimento público no momento da revelação, exceto se isso tal fato decorrer de ato ou omissão da CONTRATADA;
II - já esteja em poder da CONTRATADA, como resultado de sua própria pesquisa, contanto que a CONTRATADA possa comprovar referido fato; ou
III - tenha sido comprovada e legitimamente recebida de terceiros, estranhos à relação contratual, contanto que a CONTRATADA possa comprovar referido fato.

4. CLÁUSULA QUARTA - DAS OBRIGAÇÕES
A CONTRATADA se obriga a manter sigilo de toda e qualquer informação definida neste TERMO DE CONFIDENCIALIDADE como confidencial, utilizando-as exclusivamente para os propósitos do contrato.

Subcláusula Primeira - A CONTRATADA determinará a observância deste TERMO DE CONFIDENCIALIDADE a todos os seus empregados, prepostos e prestadores de serviço que estejam direta ou indiretamente envolvidos com a execução do contrato.

Subcláusula Segunda - A CONTRATADA obriga-se a informar imediatamente à PGDF qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

Subcláusula Terceira - Compromete-se, ainda, a CONTRATADA a não revelar, reproduzir ou utilizar, bem como não permitir que seus empregados, prepostos ou prestadores de serviço revelem, reproduzam ou utilizem, em hipótese alguma, as informações referidas no presente TERMO DE CONFIDENCIALIDADE como confidenciais, ressalvadas situações previstas no contrato e neste TERMO DE CONFIDENCIALIDADE.

Subcláusula Quarta - A CONTRATADA deve cuidar para que as informações consideradas confidenciais nos termos do presente TERMO DE CONFIDENCIALIDADE fiquem restritas ao conhecimento dos empregados, prepostos ou prestadores de serviço que estejam diretamente envolvidos nas discussões, análises, reuniões e negócios, devendo cientificá-los da existência deste TERMO DE CONFIDENCIALIDADE e da natureza confidencial das informações.

5. CLÁUSULA QUINTA - DO RETORNO DAS INFORMAÇÕES
A CONTRATADA devolverá imediatamente à PGDF, ao término do Contrato, todo e qualquer material de propriedade desta, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial, nos termos do presente TERMO DE ONFIDENCIALIDADE, a que teve acesso em decorrência do vínculo contratual com a PGDF.

6. CLÁUSULA SEXTA - DO DESCUMPRIMENTO
O descumprimento de qualquer cláusula deste TERMO DE CONFIDENCIALIDADE acarretará as responsabilidades civil, criminal e administrativa, conforme previsto na legislação.

7. CLÁUSULA SÉTIMA - DA VIGÊNCIA
Tendo em vista o princípio da boa-fé objetiva, permanece em vigor o dever de sigilo, tratado no presente TERMO DE CONFIDENCIALIDADE, após o término do Contrato.

8. CLÁUSULA OITAVA - DAS DISPOSIÇÕES FINAIS
Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pela PGDF.
Por estar de acordo, a CONTRATADA, por meio de seu representante, firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

Brasília, DF, de de 2015.

<table>
<tr><td colspan="2"><REPRESENTANTE DA CONTRATADA>

<VÍNCULO DO REPRESENTANTE COM A CONTRATADA>

RG:

CPF:</td></tr>
<tr><td>DE ACORDO:
(Integrante da equipe técnica da CONTRATADA)

_____

Nome:

RG:</td><td>DE ACORDO:
(Integrante da equipe técnica da CONTRATADA)

_____

Nome:

RG:</td></tr>
</table>

ANEXO VIII

MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO	
IDENTIFICAÇÃO	
Contrato: **Processo:** **Empenho:** **Objeto:** **PGDF:** **EMPRESA:**	**Nº do Ofício / Memorando / Documento:**
Por este instrumento, atestamos para fins de cumprimento do disposto no artigo 73 da Lei nº 8.666/93, conforme artigo 25, inciso III, alínea "a" da Instrução Normativa SLTI nº 4/2010, que os serviços (ou bens), relacionados no Ofício/Memorando/Documento acima identificada, foram recebidos nesta data e serão objeto de avaliação quanto aos aspectos de qualidade, de acordo com os Critérios de Aceitação previamente definidos pela PGDF no Termo de Referencia, anexo I do Edital. Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até xx dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência correspondente ao Contrato supracitado.	
DE ACORDO	
PGDF **Fiscal Técnico do Contrato** _____ ***<Nome>*** **Mat.:**	**EMPRESA** **Preposto** _____ ***<Nome>*** **Mat.:**

Brasília, _____ de _____ de 20____

ANEXO IX

MODELO DE TERMO DE RECEBIMENTO DEFINITIVO	
IDENTIFICAÇÃO	
Contrato: **Processo:** **Empenho:** **Objeto:** **PGDF:** **EMPRESA:**	**Nº do Ofício / Memorando / Documento:**
Por este instrumento, as partes acima identificadas atestam para fins de cumprimento do disposto no artigo 73 da Lei 8.666/93, conforme artigo 25, inciso III, alínea "h" da Instrução Normativa SLTI nº 4/2010, que os serviços (ou bens), identificados acima possuem a qualidade compatível com a especificada no Termo de Referência correspondente ao Contrato supracitado.	
DE ACORDO	
PGDF **Fiscal Técnico do Contrato** _____ ***<Nome>*** **Mat.:**	**EMPRESA** **Preposto** _____ ***<Nome>*** **Mat.:**

Brasília, _____ de _____ de 20____

ANEXO X

MINUTA DO CONTRATO

Contrato de Prestação de Serviços nº ___/___ - ___, nos termos do Padrão nº 01/2002.
Processo nº _____.

CLÁUSULA PRIMEIRA – DAS PARTES
O Distrito Federal, por meio da Procuradoria-Geral do Distrito Federal, representada por _____, na qualidade de _____, com delegação de competência prevista nas Normas de Execução Orçamentária, Financeira e Contábil do Distrito Federal e _____, doravante denominada Contratada, CGC nº _____, com sede em _____, representada por _____, na qualidade de _____.

CLÁUSULA SEGUNDA – DO PROCEDIMENTO
O presente Contrato obedece aos termos do Edital de _____ nº _____ (fls. _____), da Proposta de fls. _____ , da Lei nº 8.666 21.06.93 e 10.520/2005, Decreto Federal nº 5.450/2005 e Decreto Distrital nº 23.460/2002.

CLÁUSULA TERCEIRA – DO OBJETO
Contratação de empresa para fornecimento de solução de segurança de rede, composta por 6 (seis) *firewalls appliances*, sistema de gerencia e monitoração centralizada, serviços de instalação e configuração, transferência de conhecimento, garantia e suporte técnico on-site, consoante especifica o Edital de _____ nº _____ (fls. ____), seus anexos e a Proposta de fls. _____, que passam a integrar o presente Termo.

CLÁUSULA QUARTA – DA FORMA E REGIME DE EXECUÇÃO
O Contrato será executado de forma indireta, sob o regime de empreitada por preço global, segundo o disposto nos arts. 6º e 10º da Lei nº 8.666/93.

CLÁUSULA QUINTA – DO VALOR
5.1. O valor total do contrato é de _____(_____), conforme detalhamento abaixo, procedente do Orçamento do Distrito Federal para o corrente exercício, nos termos da correspondente Lei Orçamentária Anual, enquanto a parcela remanescente se houver, será custeada à conta de dotações a serem alocadas no(s) orçamento(s) seguinte(s).

SOLUÇÃO PARA FIREWALL						
ITEM	**SUBITEM**	**BEM / SERVIÇO**	**QTDE**	**Un.**	**VALOR UNITÁRIO - R$**	**VALOR TOTAL - R$**
1	**1.1**	Firewall Appliance Tipo 1	**2**	**Solução**		
	1.2	Firewall Appliance Tipo 2	**2**	**Solução**		
	1.3	Firewall Appliance Tipo 3	**2**	**Solução**		
	1.4	Gerência e Monitoração Centralizada	**1**	**Sistema**		
	1.5	Instalação e Configuração	**1**	**Serviço**		
	1.6	Transferência de Conhecimento	**1**	**Turma**		
	1.7	Suporte Técnico	**48**	**Meses**		
TOTAL						

5.2.O valor deste contrato será fixo e irreajustável.

CLÁUSULA SEXTA – DA DOTAÇÃO ORÇAMENTÁRIA

6.1 – A despesa correrá à conta da seguinte Dotação Orçamentária:

I – Unidade Orçamentária: 120901- FUNDO DA PROCURADORIA-GERAL DO DF

II – Programa de Trabalho: 03.126.6003.1471.0034 e 03.126.6003.2557.0019

III – Natureza da Despesa: 44.90.52 e 33.90.39

6.2 – O empenho inicial é de _____ (_____), conforme Nota de Empenho nº _____, emitida em _____, sob o evento nº _____, na modalidade _____.

CLÁUSULA SÉTIMA – DO PAGAMENTO

7.1. O pagamento será realizado, de acordo com as Normas de Execução Orçamentária, Financeira e Contábil do Distrito Federal, em até 30 (trinta) dias, contados a partir da data de apresentação da Nota Fiscal/Fatura, devidamente atestada pelo Executor do Contrato, desde que o documento de cobrança esteja em condições de liquidação e pagamento, sendo que:

7.1.1 para a **solução de segurança da informação** (*firewalls appliance*s, sistema de gerencia e monitoração, serviços de instalação e configuração, passagem de conhecimento) o pagamento **será integral,** de acordo com o estabelecido no **item 6.7.1** do Termo de Referência, anexo I do Edital**;**

7.1.2. para o **serviço de suporte técnico o pagamento** será efetuado **mensalmente**, somente após o recebimento definitivo da solução, conforme item 6.7.2 do Termo de Referência.

7.2. Para efeito de pagamento, a PGDF consultará os sítios oficiais dos órgãos e entidades emissores das certidões a seguir relacionadas, **para a verificação da regularidade fiscal da Contratada:**

a) **Certidão de regularidade** de débitos Relativos às **Contribuições Previdenciárias** e às de Terceiros, expedida pela Secretaria da Receita Federal do Brasil (Decreto Federal nº 6.106/2007);

b) Certificado de **Regularidade do Fundo de Garantia por Tempo de Serviço** – FGTS, fornecido pela CEF – Caixa Econômica Federal, devidamente atualizado (Lei n.º 8.036/90);

c) Certidão de **Regularidade** com **a Fazenda do Distrito Federal.**

d) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de **Certidão Negativa de Débitos Trabalhistas** – **CNDT** (Lei nº 12.440, de 7 de julho de 2011).

7.2.1. Em havendo a impossibilidade de consulta, pela Administração, aos sítios oficiais dos órgãos e entidades emissores das citadas certidões, o pagamento ficará condicionado à apresentação, pela **Contratada, da comprovação de sua regularidade fiscal e trabalhista.**

7.2.2. A Contratada deverá observar o disposto na Lei nº 5.087 de 25.03.2013 do Distrito Federal.

CLÁUSULA OITAVA – DO PRAZO DE VIGÊNCIA

A **vigência deste contrato será de 51 (cinquenta e um) meses**, a contar da data de sua assinatura, com eficácia a partir de sua publicação, compreendendo os prazos de entrega dos equipamentos, de procedimentos de recebimento fixados, da instalação e configuração da solução, passagem de conhecimento, bem como da garantia, onde neste caso, iniciar-se-á a contagem a partir do recebimento definitivo da solução.

CLÁUSULA NONA – DAS GARANTIAS

9.1. DA GARANTIA CONTRATUAL

9.1.2. .Para o fiel cumprimento das obrigações contratuais, a contratada prestará garantia no valor correspondente a 5% (cinco por cento) do montante do contrato, mediante a seguinte modalidade ---------- conforme previsão constante do Edital.

9.1.3. O adjudicatário convocado deve apresentar, no prazo máximo de 10 (dez) dias úteis, contado da data da entrega da via do contrato assinada, comprovante de prestação de garantia no valor e nas condições descritas no Edital.

9.1.4. A garantia somente poderá ser levantada após o cumprimento integral de todas as obrigações contratuais assumidas e a extinção do Contrato;

9.1.5. A garantia ficará retida no caso de rescisão contratual por responsabilidade da Contratada, até a definitiva solução das pendências administrativas ou judiciais que porventura existam.

9.1.6. Sem prejuízo das sanções previstas na lei e neste Edital, a não prestação da garantia exigida será considerada inexecução do Contrato, implicando na imediata anulação da Nota de Empenho emitida e ensejará a rescisão Contratual, nos termos do inciso I do art. 78 da Lei nº 8.666/93.

9.2. DA GARANTIA DA SOLUÇÃO E SUPORTE TÉCNICO

9.2.1. O garantia e suporte técnico dos componentes da solução deverá ser realizada de forma on-site, ou seja, no local. A garantia e suporte técnico deverá ser prestada pelo prazo de **48 (quarenta e oito) meses,** contados da data do seu recebimento definitivo;

9.2.2. Os equipamentos deverão ter garantia e assistência técnica no local onde serão instalados pelo período estipulado no item anterior, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

9.2.3. Durante todo o período de garantia está incluído a atualização tecnológica de todas as licenças e softwares presentes na solução, sem nenhum ônus adicional para a PGDF;

9.2.4. O suporte técnico deve manter o equipamento sempre atualizado com a última versão do firmware, porém a atualização deverá ocorrer de forma planejada – formalizada por um plano de mudanças.

9.2.5. Independentemente da aceitação, a contratada garantirá a qualidade de cada unidade do equipamento fornecido pelo prazo estabelecido de no mínimo 48 (quarenta e oito) meses, obrigando-se a repor aquele que apresentar defeito:

9.2.5.1. Se algum dos equipamento da solução apresentar defeito, o mesmo deverá ser trocado imediatamente por outro equipamento de forma provisória, de qualidade igual ou superior, que atenda todos os requisitos estabelecidos neste Termo de Referência no prazo máximo de 4 (quatro) horas, e este equipamento que apresentou defeito deverá ser consertado em um prazo máximo de 30 dias;

9.2.6. A contratada deverá prover uma central de atendimento gratuito ou com custo de ligação local, para realizar abertura de chamados mediante a utilização dos seguintes meios de comunicação:

9.2.6.1. Telefone: 24 horas por dia, 7 dias por semana e 365 dias por ano;

9.2.6.2. E-mail e internet: 24 horas por dia, 7 dias por semana e 365 dias por ano;

9.2.7. A central de atendimento deve possuir software na web ou enviar por e-mail o status do chamado e histórico contínuo do atendimento. Deve possuir meio para que a CONTRATANTE controle mensalmente e anualmente, dentro do período de vigência do contrato, os relatórios estatísticos, os chamados abertos, em atendimento, concluídos etc.

9.2.8. A PGDF fará a “Abertura de Chamados Técnicos” que deverão obedecer os prazos de atendimento estipulados abaixo:

Severidade	Descrição	Prazo de Solução Definitiva
ALTA	Este nível de severidade é aplicado quando há indisponibilidade no uso dos serviços.	4 (quatro) horas
MÉDIA	Este nível de severidade é aplicado quando há falha, simultânea ou não, no uso dos serviços, estando ainda disponíveis, porém apresentando problemas.	6 (seis) horas
BAIXA	Este nível de severidade é aplicado para problemas que não afetem o desempenho e disponibilidade dos serviços, bem como para atualizações de software do roteador, esclarecimentos técnicos relativos ao uso e aprimoramento dos serviços. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados.	5 (cinco) dias úteis

9.2.9. Será considerado para efeitos do nível de serviço exigido, prazo de solução definitiva, como o tempo decorrido entre a abertura do chamado técnico efetuada pela equipe técnica da PGDF à Contratada e a efetiva recolocação dos serviços em seu pleno estado de funcionamento e consequentemente resolução do problema;

9.2.10. Depois de concluído a resolução do chamado referente ao pedido de suporte, a Contratada comunicará o fato à equipe técnica da PGDF e solicitará autorização para o fechamento do chamado. Caso a PGDF não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela Contratada. Neste caso, a PGDF fornecerá as pendências relativas ao chamado aberto;
9.2.11. A CONTRATADA deverá disponibilizar pelo Portal de Atendimento ou por E-mail, uma forma de acompanhamento dos serviços contratados.
9.2.12. Entende-se como Portal de Atendimento, qualquer ferramenta de gerência acessível através da Internet por intermédio de um navegador Web, com acesso restrito através de usuário/senha eletrônica.
9.2.13. O Portal de Atendimento deverá possuir informações de estatísticas do desempenho da rede, consulta aos históricos dos registros das ocorrências e registros de solicitações e reclamações enviadas pela PGDF;
9.2.14. A CONTRATADA deverá fornecer pelo menos um usuário/senha para acessar o Portal de Atendimento dos Serviços. O Portal de Atendimento poderá ser substituído pelo E-mail, conforme tópico 5.5.11;
9.2.15. Geração de relatórios online (mensal e anual) com histórico de chamados abertos pela PGDF;
9.2.16. Possuir meios de auditoria de todos os serviços, possibilitando que a PGDF possa sempre que desejar, comprovar a qualidade e eficácia dos serviços oferecidos;
9.2.17. Deverá ser fornecido mensalmente, juntamente com a Nota Fiscal, o relatório detalhado contendo todos os registros de chamados técnicos abertos no referido período;
9.2.18. Deve ser informado link (URL) de site na internet do fabricante dos equipamentos com disponibilidade de informações para suporte, tais como: guia de instalação, informações técnicas, atualização e download de drives, firmwares upgrade de BIOS.

CLÁUSULA DÉCIMA – DA RESPONSABILIDADE DO DISTRITO FEDERAL

10.1. O Distrito Federal responderá pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo e de culpa.
10.2. Constitui obrigações da Contratante:
10.2.1. Indicar o executor contrato, conforme art. 67, da Lei n° 8.666/1993.
10.2.2. Promover o acompanhamento e a fiscalização do recebimento e da execução do objeto contratual objetivando o seu perfeito cumprimento, sob os aspectos quantitativo e qualitativo, registrando as falhas detectadas.
10.2.3. Proporcionar todas as facilidades para que a Contratada possa efetuar os serviços dentro das normas estabelecidas no contrato;
10.2.4. Permitir livre acesso aos funcionários da Contratada aos equipamentos, objeto deste contrato, para execução dos serviços de instalação, configuração, garantia e suporte técnico;
10.2.5. Receber os equipamentos e serviços entregues pela CONTRATADA, desde que estejam em conformidade com o objeto contratado;
10.2.6 Prestar informações e esclarecimentos que venham a ser solicitados pela CONTRATADA;
10.2.7. Notificar à CONTRATADA sobre imperfeições, falhas ou irregularidades constatadas nos equipamentos e serviços, para que sejam adotadas as medidas necessárias;
10.2.8. Solicitar de imediato a pronta reparação, substituição de equipamentos mantendo a qualidade do objeto contratado, ou parte, que se apresente com defeito ou em desacordo com a especificação descrita em contrato;
10.2.9. Efetuar os pagamentos devidos nos prazos previstos desde que cumprida as obrigações contratuais.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

11.1 – Apresentar, ao Distrito Federal:
I – até o quinto dia útil do mês subsequente, comprovante de recolhimento dos encargos previdenciários, resultantes da execução do Contrato;
II – comprovante de recolhimento dos encargos trabalhistas, fiscais e comerciais.
11.2 –Constitui obrigações da Contratada:
11.2.1. O pagamento dos salários e demais verbas decorrentes da prestação de serviço.
11.2.2 – Responder pelos danos causados por seus agentes.
11.2.3 – Manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

11.2.4.Cumprir fielmente as obrigações assumidas constantes do Edital de Licitação, do Contrato e da Proposta, de forma que os serviços sejam realizados com esmero e perfeição;
11.2.5. Fornecer por sua conta e responsabilidade os equipamentos, softwares, licenças (e qualquer outro material necessário para a configuração e ativação da solução), serviços de instalação, configuração e passagem de conhecimento necessários ao funcionamento e operação da solução, bem como prestar o serviço de garantia e assistência técnica, conforme as especificações, níveis de qualidade e prazos contratados, e assim mantê-los por todo o período de garantia;
11.2.6. Reunir-se com a PGDF para levantar as necessidades de projeto de acordo com os prazos e regras definidas no Termo de Referência e seus anexos;
11.2.7. Entregar o projeto de implantação da solução de acordo com os prazos e regras definidas no Termo de Referência e seus anexos;
11.2.8.Realizar a instalação e configuração dos equipamentos conforme especificações contidas no Termo de Referência e seus anexos;
11.2.9. Realizar as movimentações dos equipamentos conforme prazos e especificações contidas no Termo de Referência e seus anexos;
11.2.10. Efetuar transferência de conhecimento para os colaboradores indicados pela Diretoria de Organização e Sistemas (DISIS) de modo que eles sejam capazes de configurar e operar o equipamento e conforme especificações do Termo de Referência e seus anexos;
11.2.11. Cumprir os prazos de resolução de chamados definidos para a fase de instalação e configuração da solução;
11.2.12.Cumprir os prazos de resolução de chamados definidos para a fase de garantia e suporte técnico da solução;
11.2.13.**Apresentar comprovação de que empresa possui em seu corpo técnico, pelo menos 01 (um) técnico com certificação oficial fornecida pelo(s) fabricante(s) dos produtos o qual deverá compor a equipe que irá realizar o projeto de implantação, realizar a instalação e configuração da solução contratada e prestar o suporte técnico necessário. A comprovação do vínculo do profissional com a licitante poderá ser feito por meio de contrato social ou equivalente, carteira de trabalho ou contrato de prestação de serviços, sem vínculo trabalhista e regido pela legislação civil comum;**
11.2.14.Os equipamentos disponibilizados a Contratante deverão ser novos, de primeiro uso e estar na linha atual de produção do fabricante;
11.2.15. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas (sem quaisquer ônus para a PGDF), no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados (art.69 da Lei nº 8.666/93);
11.2.16.Assumir todos os gastos e despesas que fizer, para o adimplemento das obrigações decorrentes do Contrato;
11.2.17. Providenciar junto à PGDF a identificação dos seus empregados, os quais deverão porta-se adequadamente nas dependências da PGDF;
11.2.18.Responder por todos os encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução do objeto contratado, vez que seus empregados não terão qualquer vínculo empregatício com a Contratante;
11.2.19.Não causar qualquer dano à estrutura física da PGDF;
11.2.20. Ressarcir ao Contratante quaisquer danos ou prejuízos causados à Administração em decorrência da execução dos serviços.
11.2.21.Não transferir a terceiro, por qualquer forma, nem mesmo parcialmente, o objeto deste contrato;
11.2.22. A Contratada deverá assinar TERMO DE CONFIDENCIALIDADE e manter sigilo de todos os dados ou informações da Contratante ou de suas representações obtidas em função da prestação do serviço contratado, conforme definido no subtópico "**6.8 DO SIGILO"**;
11.2.23. Obriga-se a aceitar, nas mesmas condições contratuais, e mediante Termo Aditivo, os acréscimos ou supressões que se fizerem necessários, no montante de até 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato, de acordo com os Parágrafos Primeiro e Segundo do Artigo 65 da Lei nº 8.666/93.
11.2.24. As funcionalidades do firewall, de IPS, antivírus e *anti-spyware* devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
11.2.25. Não fazer uso de mão de obra infantil, nos termos da Lei Distrital nº 5.061/2013.
11.2.26.Adotar na execução dos serviços, práticas de sustentabilidade ambiental, a recepção de bens, embalagens, recipientes ou equipamentos inservíveis e não reaproveitáveis pela PGDF, práticas de desfazimento sustentável,

reciclagem dos bens inservíveis e processos de reutilização, nos termos estabelecidos na Lei Distrital nº 4.770, de 22 de fevereiro de 2012, que sejam aplicáveis ao objeto deste contrato.

CLÁUSULA DÉCIMA SEGUNDA – DA ALTERAÇÃO CONTRATUAL

12.1 – Toda e qualquer alteração deverá ser processada mediante a celebração de Termo Aditivo, com amparo no art. 65 da Lei nº 8.666/93, vedada a modificação do objeto.

12.2 – A alteração de valor contratual, decorrente de compensação ou penalização financeira, prevista no Contrato, bem como o empenho de dotações orçamentárias, suplementares, até o limite do respectivo valor, dispensa a celebração de aditamento.

CLÁUSULA DÉCIMA TERCEIRA – DAS PENALIDADES

13.1. O atraso injustificado na execução, bem como a inexecução total ou parcial do Contrato sujeitará a Contratada as sanções específicas, previstas no Termo de Referência, anexo I do edital, transcritas abaixo, além das previstas no Edital, estabelecidas o Decreto nº 26.851, de 30/05/2006, publicado no DODF nº 103, de 31/05/2006, pg. 05/07, com suas alterações.

13.1.1. Sanções Aplicáveis

13.1.1.1. As multas deverão ser aplicadas à Contratada, em caso de descumprimento das cláusulas, conforme planilha abaixo:

TABELA 1 - PERCENTAGEM	
GRAU	%
1	0,025
2	0,030
3	0,10
4	0,25
5	0,50
6	0,75
7	1,0
8	1,1

TABELA 2 – INFRAÇÃO/GRADUAÇÃO		
N.	**INFRAÇÃO**	GRAU
1	**Descrição:** Descumprimento do prazo de entrega dos equipamentos, conforme estabelecido no subtópico “6.5.1 Da Entrega dos Equipamentos”. **Unidade Temporal:** % por dia, limitado a 15 (quinze) dias de atraso. **Correspondência:** sobre o valor dos equipamentos.	3
2	Descumprimento do prazo de reunião com a PGDF afim de levantar as necessidades de projeto para subsidiar a elaboração do projeto de implantação da solução, conforme prazo estabelecido no subtópico “6.5.2	4

	Do Projeto de Implantação da Solução". **Unidade Temporal:** % por dia, limitado a 15 (quinze) dias de atraso. **Correspondência:** sobre o valor da instalação e configuração da solução.	
3	Descumprimento do prazo de entrega do projeto de implantação da solução, conforme prazo estabelecido no subtópico "6.5.2 Do Projeto de Implantação da Solução". **Unidade Temporal:** % por dia, limitado a 15 (quinze) dias de atraso. **Correspondência:** sobre o valor da instalação e configuração da solução.	6
4	Descumprimento do prazo de início da passagem de conhecimento, conforme estabelecido no subtópico "6.5.3 Da Passagem de Conhecimento"; **Unidade Temporal:** % por dia, limitado a 20 (vinte) dias de atraso. **Correspondência:** sobre o valor da passagem de conhecimento da solução.	8
5	Descumprimento do prazo de instalação e configuração da solução, conforme estabelecido no subtópico "6.5.4 Da Instalação e Configuração". **Unidade Temporal:** % por dia, limitado a 15 (quinze) dias de atraso. **Correspondência:** sobre o valor da instalação e configuração da solução.	7
6	Descumprimento do prazo de movimentação e sua respectiva reinstalação (caso precise) dos equipamentos, conforme estabelecido no subtópico "5.4.3". **Unidade Temporal:** % por dia, limitado a 20 (vinte) dias de atraso. **Correspondência:** sobre o valor da instalação e configuração da solução.	5
7	Descumprimento do prazo de atendimento de suporte técnico, conforme estabelecido no tópico "5.5 Da Garantia e Suporte Técnico", na resolução do problema. **Unidade Temporal:** % por hora, limitado à 48 (quarenta e oito) horas de atraso. **Correspondência:** sobre o valor total do contrato.	1
8	Descumprimento dos prazos de entrega de relatório mensal, conforme estabelecido no subtópico "5.5.17"; **Unidade Temporal:** % por dia, limitado à 15 (quinze) dias de atraso. **Correspondência:** sobre o valor total do contrato;	2

13.1.1.2. Para fins de comprovação de tempo para aplicação das multas referente às infrações de número 7, considera-se como 1 (uma) hora inteira a fração igual ou superior 30 minutos;

CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO AMIGÁVEL

O Contrato poderá ser rescindido por acordo entre as partes, reduzido a termo no processo da licitação, desde que haja conveniência para a Administração, devendo para tanto, o ato ser precedido de autorização escrita e fundamentada da autoridade competente.

CLÁUSULA DÉCIMA QUINTA – DA RESCISÃO

O Contrato poderá ser rescindido por ato unilateral da Administração, reduzido a termo no respectivo processo, na forma prevista no Edital, observado o disposto no art. 78 da Lei nº 8.666/93, sujeitando-se a Contratada às consequências determinadas pelo art. 80 desse diploma legal, sem prejuízo das demais sanções cabíveis.

CLÁUSULA DÉCIMA SEXTA – DOS DÉBITOS PARA COM A FAZENDA PÚBLICA

Os débitos da Contratada para com o Distrito Federal, decorrentes ou não do ajuste, serão inscritos em Dívida Ativa e cobrados mediante execução na forma da legislação pertinente, podendo, quando for o caso, ensejar a rescisão unilateral do Contrato.

CLÁUSULA DÉCIMA SÉTIMA – DO EXECUTOR

O Distrito Federal, por meio de _____, designará um Executor para o Contrato, que desempenhará as atribuições previstas nas Normas de Execução Orçamentária, Financeira e Contábil.

CLÁUSULA DÉCIMA OITAVA - DA PUBLICAÇÃO E DO REGISTRO

A eficácia do Contrato fica condicionada à publicação resumida do instrumento pela Administração, na Imprensa Oficial, até o quinto dia útil do mês seguinte ao de sua assinatura, para ocorrer no prazo de vinte dias daquela data, após o que deverá ser providenciado o registro do instrumento no órgão interessado, de acordo com o art. 60 da Lei nº 8.666/93.

CLÁUSULA DÉCIMA NONA – DO FORO

19.1. Havendo irregularidades neste instrumento, entre em contato com a Ouvidoria de Combate à Corrupção, no telefone 0800-6449060. (Decreto nº 34.031/2012, publicado no DODF de 13/12/2012 p 5.)

19.2. Fica eleito o foro de Brasília, Distrito Federal, para dirimir quaisquer dúvidas relativas ao cumprimento do presente Contrato.

Brasília, _____ de _____ de 20__

Pelo Distrito Federal:
Pela Contratada:
Testemunhas:
01. ----------
02. ----------

ANEXO XI

DAS PENALIDADES

DECRETO Nº 26.851, DE 30 DE MAIO DE 2006.

Regula a aplicação de sanções administrativas previstas nas Leis Federais nos 8.666, de 21 de junho de 1993 (Lei de Licitações e Contratos Administrativos), e 10.520, de 17 de julho de 2002 (Lei do Pregão), e dá outras providências.

A GOVERNADORA DO DISTRITO FEDERAL, no uso das atribuições que lhe confere o artigo 100, inciso VII, da Lei Orgânica do Distrito Federal, e tendo em vista o disposto nos artigos 81, 86, 87 e 88 da Lei Federal n° 8.666, de 21 de junho de 1993, e no art. 7° da Lei Federal n° 10.520, de 17 de julho de 2002, bem como o disposto no art. 68 da Lei Federal n° 9.784, de 29 de janeiro de 1999, e ainda, a centralização de compras instituída nos termos da Lei Distrital n° 2.340, de 12 de abril de 1999, e as competências instituídas pela Lei Distrital n° 3.167, de 11 de julho de 2003, DECRETA:

CAPÍTULO I

DAS SANÇÕES ADMINISTRATIVAS

SEÇÃO I

Disposições Preliminares

Art. 1° A aplicação das sanções de natureza pecuniária e restritiva de direitos pelo não comprimento das normas de licitação e/ou de contratos, em face do disposto nos arts. 81, 86, 87 e 88, da Lei Federal n° 8.666, de 21 de junho de 1993, e no art. 7° da Lei Federal n° 10.520, de 17 de julho de 2002, obedecerá, no âmbito da Administração Direta, Autárquica, Fundacional e das Empresas Públicas do Distrito Federal, às normas estabelecidas no presente decreto.

Parágrafo único. As disposições deste Decreto aplicam-se também aos ajustes efetuados com dispensa e inexigibilidade de licitação, nos termos do que dispõe a legislação vigente, e ainda às licitações realizadas pelas Administrações Regionais, até o limite máximo global mensal estabelecido no art. 24, incisos I e II, da Lei Federal n° 8.666.

SEÇÃO II

Das Espécies de Sanções Administrativas

Art. 2° As licitantes que não cumprirem integralmente as obrigações contratuais assumidas, garantida a prévia defesa, estão sujeitas às seguintes sanções:

I - advertência;

II – multa;

III - suspensão temporária de participação em licitação, e impedimento de contratar com a Administração do Distrito Federal:

a) para o licitante e/ou contratado através da modalidade pregão presencial ou eletrônico que, convocado dentro do prazo de validade de sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução do seu objeto, comportar-se de modo inidôneo ou cometer fraude fiscal; a penalidade será aplicada por prazo não superior a 5 (cinco) anos, e o licitante e/ou contratado será descredenciado do Sistema de Cadastro de Fornecedores, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, aplicadas e dosadas segundo a natureza e a gravidade da falta cometida;

b) para os licitantes nas demais modalidades de licitação previstas na Lei n. 8.666, de 1993, a penalidade será aplicada por prazo não superior a 2 (dois) anos, e dosada segundo a natureza e a gravidade da falta cometida.

IV - declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

Parágrafo único. As sanções previstas nos incisos I, III e IV deste artigo poderão ser aplicadas juntamente com a do inciso II, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 5 (cinco) dias úteis.

SUBSEÇÃO I

Da Advertência

Art. 3° A advertência é o aviso por escrito, emitido quando o licitante e/ou contratado descumprir qualquer obrigação, e será expedido:

I - pela Subsecretaria de Compras e Licitações - SUCOM, quando o descumprimento da obrigação ocorrer no âmbito do procedimento licitatório, e, em se tratando de licitação para registro de preços, até a emissão da autorização de compra para o órgão participante do Sistema de Registro de Preços;

II - pelo ordenador de despesas do órgão contratante e/ou participante do Sistema de Registro de Preços, se o descumprimento da obrigação ocorrer na fase de execução contratual, entendida desde a recusa em retirar a nota de empenho ou assinar o contrato.

SUBSEÇÃO II

Da Multa

Art. 4° A multa é a sanção pecuniária que será imposta ao contratado pelo atraso injustificado na entrega ou execução do contrato, e será aplicada nos seguintes percentuais:

I - 0,33% (trinta e três centésimos por cento) por dia de atraso, na entrega de material ou execução de serviços, calculado sobre o montante das parcelas obrigacionais adimplidas em atraso, até o limite de 9,9% (nove inteiros e nove décimos por cento), que corresponde a até 30 (trinta) dias de atraso; (Redação dada pelo Decreto 35.831, de 19/09/2014, DODF de 22/09/2014 p 6)

II - 0,66 % (sessenta e seis centésimos por cento) por dia de atraso, na entrega de material ou execução de serviços, calculado, desde o primeiro dia de atraso, sobre o montante das parcelas obrigacionais adimplidas em atraso, em caráter excepcional, e a critério do órgão contratante, quando o atraso ultrapassar 30 (trinta) dias, não podendo ultrapassar o valor previsto para o inadimplemento completo da obrigação contratada[1] **(Redação dada pelo Decreto 35.831, de 19/09/2014 , DODF de 22/09/2014 p 6)**

III - 5% (cinco por cento) sobre o valor total do contrato/nota de empenho, por descumprimento do prazo de entrega, sem prejuízo da aplicação do disposto nos incisos I e II deste artigo;

IV - 15% (quinze por cento) em caso de recusa injustificada do adjudicatário em assinar o contrato ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Administração, recusa parcial ou total na entrega do material, recusa na conclusão do serviço, ou rescisão do contrato/ nota de empenho, calculado sobre a parte inadimplente;

V [2]- até 20% (vinte por cento) sobre o valor do contrato/nota de empenho, pelo descumprimento de qualquer cláusula do contrato, exceto prazo de entrega. **(Redação dada pelo Decreto 35.831, de 19/09/2014, DODF de 22/09/2014 p 6)**

§ 1º A multa será formalizada por simples apostilamento contratual, na forma do art. 65, § 8º, da Lei nº 8.666, de 193 e será executada após regular processo administrativo, oferecido ao contratado a oportunidade de defesa prévia, no prazo de 05 (cinco) dias úteis, a contar do recebimento da notificação, nos termos do § 3o do art. 86 da Lei nº 8.666, de 1993, observada a seguinte ordem:

I - mediante desconto no valor da garantia depositada do respectivo contrato;

II - mediante desconto no valor das parcelas devidas ao contratado;

III - mediante procedimento administrativo ou judicial de execução.

§ 2º Sempre que a multa ultrapassar os créditos do contratado e/ou garantias, o seu valor será atualizado, a partir da data da aplicação da penalidade, pela variação do Índice Geral de Preços - Mercado (IGP-M), da Fundação Getúlio Vargas.

§ 3º O atraso, para efeito de cálculo de multa, será contado em dias corridos, a partir do dia seguinte ao do vencimento do prazo de entrega ou execução do contrato, se dia de expediente normal na repartição interessada, ou no primeiro dia útil seguinte.

§ 4º Em despacho, com fundamentação sumária, poderá ser relevado:

I - o atraso não superior a 5 (cinco) dias;

II - a execução de multa cujo montante seja inferior ao dos respectivos custos de cobrança.

§ 5º A multa poderá ser aplicada cumulativamente com outras sanções, segundo a natureza e a gravidade da falta cometida, consoante o previsto no Parágrafo único do art. 2º e observado o princípio da proporcionalidade.

§ 6º Decorridos 30 (trinta) dias de atraso, a nota de empenho e/ou contrato deverão ser cancelados e/ou rescindidos, exceto se houver justificado interesse da unidade contratante em admitir atraso superior a 30 (trinta) dias, que será penalizado na forma do inciso II do caput deste artigo.

§ 7º A sanção pecuniária prevista no inciso IV do caput deste artigo não se aplica nas hipóteses de rescisão contratual que não ensejam penalidades.

SUBSEÇÃO III

Da Suspensão

Art. 5° A suspensão é a sanção que suspende temporariamente a participação de contratado em licitações e o impede de contratar com a Administração, e, se aplicada em decorrência de licitação na modalidade pregão, ainda suspende o registro cadastral do adjudicado e/ou contratado, no Cadastro de Fornecedores do Distrito Federal, instituído pelo Decreto nº 25.966, de 23 de junho de 2005, com a suspensão inscrita no Sistema de Cadastramento Unificado de Fornecedores -SICAF, de acordo com os prazos a seguir:

I - por até 30 (trinta) dias, quando, vencido o prazo de advertência, emitida pela Subsecretaria de Compras e Licitações, ou pelo órgão integrante do Sistema de Registro de Preços, a empresa permanecer inadimplente;

II - por até 90 (noventa) dias, em licitação realizada na modalidade pregão presencial ou eletrônico, ou pregão para inclusão no Sistema de Registro de Preços, quando a licitante deixar de entregar, no prazo estabelecido no edital, os documentos e anexos exigidos, quer por via fax ou internet, de forma provisória, ou, em original ou cópia autenticada, de forma definitiva;

III - por até 12 (doze) meses, quando a licitante, na modalidade pregão, convocada dentro do prazo de validade de sua proposta, não celebrar o contrato, ensejar o retardamento na execução do seu objeto, falhar ou fraudar na execução do contrato;

IV - por até 24 (vinte e quatro) meses, quando a licitante:

a) apresentar documentos fraudulentos, adulterados ou falsificados nas licitações, objetivando obter, para si ou para outrem, vantagem decorrente da adjudicação do objeto da licitação;

b) tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

receber qualquer das multas previstas no artigo anterior e não efetuar o pagamento; a reabilitação de dará com o pagamento.

§ 1° São competentes para aplicar a penalidade de suspensão:

I - a Subsecretaria de Compras e Licitações - SUCOM, quando o descumprimento da obrigação ocorrer no âmbito do procedimento licitatório, e, em se tratando de licitação para registro de preços, até a emissão da autorização de compra para o órgão participante do Sistema de Registro de Preços;

II - o ordenador de despesas do órgão contratante e/ou participante do Sistema de Registro de Preços, se o descumprimento da obrigação ocorrer na fase de execução contratual, entendida desde a recusa em retirar a nota de empenho ou assinar o contrato.

§ 2° A penalidade de suspensão será publicada no Diário Oficial do Distrito Federal, e produzirá os seguintes efeitos:

I - se aplicada pela Subsecretaria de Compras e Licitações - SUCOM, na hipótese do descumprimento da obrigação ocorrer no âmbito do procedimento licitatório, e, em se tratando de licitação para registro de preços, até a emissão da autorização de compra para o órgão participante do Sistema de Registro de Preços, implicará na suspensão, por igual

período, perante todos os órgãos/entidades subordinados à Lei Distrital no 2.340, de 12 de abril de 1999, e alterações posteriores;

II - se aplicada pelo ordenador de despesas do órgão contratante e/ou participante do Sistema de Registro de Preços, na hipótese do descumprimento da obrigação ocorrer na fase de execução contratual, entendida desde a recusa em retirar a nota de empenho ou assinar o contrato, implicará na suspensão perante o órgão sancionador.

§ 3° O prazo previsto no inciso IV poderá ser aumentado para até 05 (cinco) anos, quando as condutas ali previstas forem praticadas no âmbito dos procedimentos derivados dos pregões.

SUBSEÇÃO IV

Da Declaração de Inidoneidade

Art. 6° A declaração de inidoneidade será aplicada pelo Secretário de Estado de Fazenda, à vista dos motivos informados pela Subsecretaria de Compras e Licitações.

§ 1° A declaração de inidoneidade prevista neste artigo permanecerá em vigor enquanto perdurarem os motivos que determinaram a punição ou até que seja promovida a reabilitação perante a própria autoridade que a aplicou, e será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes de sua conduta e após decorrido o prazo de até dois anos de sancionamento.

§ 2° A declaração de inidoneidade e/ou sua extinção será publicada no Diário Oficial do Distrito Federal, e seus efeitos serão extensivos a todos os órgãos/entidades subordinadas ou vinculadas ao Poder Executivo do Distrito Federal, e à Administração Pública, consoante dispõe o art. 87, IV, da Lei nº 8.666, de 1993.

CAPÍTULO II

DAS DEMAIS PENALIDADES

Art. 7° As licitantes que apresentarem documentos fraudulentos, adulterados ou falsificados, ou que por quaisquer outros meios praticarem atos irregulares ou ilegalidades para obtenção no registro no Cadastro de Fornecedores do Distrito Federal, administrado pela Subsecretaria de Compras e Licitações, estarão sujeitas às seguintes penalidades:

I - suspensão temporária do certificado de registro cadastral ou da obtenção do registro, por até 24 (vinte e quatro) meses, dependendo da natureza e da gravidade dos fatos; e

II - declaração de inidoneidade, nos termos do art. 6º deste Decreto III - aplicam-se a este artigo as disposições dos §§ 2º e 3º do art. 5º deste Decreto.

Art. 8° As sanções previstas nos arts. 5º e 6º poderão também ser aplicadas às empresas ou profissionais que, em razão dos contratos regidos pelas Leis Federais nos 8.666, de 1993 ou 10.520, de 2002:

I - tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

II - tenham praticado atos ilícitos, visando frustrar os objetivos da licitação;

III - demonstrarem não possuir idoneidade para contratar com a Administração, em virtude de atos ilícitos praticados.

CAPÍTULO III

DO DIREITO DE DEFESA

Art. 9° É facultado ao interessado interpor recurso contra a aplicação das penas de advertência, suspensão temporária ou de multa, no prazo de 5 (cinco) dias úteis, a contar da ciência da respectiva notificação.

§ 1° O recurso será dirigido à autoridade superior, por intermédio da que praticou o ato recorrido, a qual poderá reconsiderar sua decisão, no prazo de 5 (cinco) dias úteis, ou, nesse mesmo prazo, fazê-lo subir, devidamente informado, devendo, neste caso, a decisão ser proferida dentro do prazo de 5 (cinco) dias úteis, contado do recebimento do recurso, sob pena de responsabilidade.

§ 2° Na contagem dos prazos estabelecidos neste Decreto, 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; só se iniciam e vencem os prazos referidos neste artigo em dia de expediente no órgão ou na entidade.

§ 3° Assegurado o direito à defesa prévia e ao contraditório, e após o exaurimento da fase recursal, a aplicação da sanção será formalizada por despacho motivado, cujo extrato deverá ser publicado no Diário Oficial do Distrito Federal, devendo constar:

I - a origem e o número do processo em que foi proferido o despacho;

II - o prazo do impedimento para licitar e contratar;

III - o fundamento legal da sanção aplicada;

IV - o nome ou a razão social do punido, com o número de sua inscrição no Cadastro da Receita Federal.

§ 4° Após o julgamento do(s) recurso(s), ou transcorrido o prazo sem a sua interposição, a autoridade competente para aplicação da sanção providenciará a sua imediata divulgação no sítio www.fazenda.df.gov.br, inclusive para o bloqueio da senha de acesso ao Sistema de Controle e Acompanhamento de Compra e Licitações e Registro de Preços do Distrito Federal – e-compras, e aos demais sistemas eletrônicos de contratação mantidos por órgãos ou entidades da Administração Pública do Distrito Federal.

§ 5° Ficam desobrigadas do dever de publicação no Diário Oficial do Distrito Federal as sanções aplicadas com fundamento nos arts. 3º e 4º deste decreto, as quais se formalizam por meio de simples apostilamento, na forma do art. 65, §8º, da Lei nº 8.666, de 1993.

CAPÍTULO IV

DO ASSENTAMENTO EM REGISTROS

Art. 10. Toda sanção aplicada será anotada no histórico cadastral da empresa.

Parágrafo único. As penalidades terão seus registros cancelados após o decurso do prazo do ato que as aplicou.

CAPÍTULO V

DA SUJEIÇÃO A PERDAS E DANOS

Art. 11. Independentemente das sanções legais cabíveis, regulamentadas por este Decreto, a licitante e/ou contratada ficará sujeita, ainda, à composição das perdas e danos causados à Administração pelo descumprimento das obrigações licitatórias e/ou contratuais.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 12. Os instrumentos convocatórios e os contratos deverão fazer menção a este Decreto, incluir os percentuais relativos a multas, e as propostas comerciais deverão mencionar expressamente a concordância do proponente aos seus termos.

Art. 13. Este Decreto entra em vigor na data de sua publicação.

Art. 14. Revogam-se as disposições em contrário.

Brasília, 30 de maio de 2006.

118º da República e 47º de Brasília

MARIA DE LOURDES ABADIA

PUBLICADO NO DODF Nº 103, DE 31 DE MAIO DE 2006 – P. 5, 6, 7.

ALTERADO PELOS DECRETOS NºS:

- 26.993, DE 12 DE JULHO DE 2006, PUBLICADO NO DODF Nº 133, DE 13 DE JULHO DE 2006, P.2.
- 27.069, DE 14 DE AGOSTO DE 2006, PULICADO NO DODF Nº 156, DE 15 DE AGOSTO DE 2006, P. 1, 2.
- 35.831, DE 19 DE SETEMBRO DE 2014, PUBLICADO NO DODF Nº 197, DE 22 DE SETEMBRO DE 2014, P. 6.