GOVERNO DO DISTRITO FEDERAL
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA DO DISTRITO FEDERAL

Havendo irregularidades neste instrumento, entre em contato com a Ouvidoria de Combate à Corrupção, no telefone 0800-6449060

MINUTA DE EDITAL

Pregão Eletrônico nº 12/2023-SSP

OBJETO: Contratação de empresa especializada para fornecer solução de segurança composta por Firewall, do tipo NGFW, de alta capacidade para Segurança de datacenter, firewalls de pequeno porte, gerência centralizada de logs e eventos dos firewall e antivírus com EDR com instalação, configuração, suporte técnico, manutenção e garantia de 36 (trinta e seis) meses, conforme especificações, quantitativos e condições estabelecidas no Termo de Referência e seus anexos.
DADOS DO PREGÃO ELETRÔNICO **MODO DE DISPUTA: ABERTO** **CRITÉRIO DE JULGAMENTO: MENOR PREÇO** **VALOR ESTIMADO: R$ SIGILOSO** **PROGRAMA DE TRABALHO:_____ Unidade Orçamentária: __ _____** **NATUREZA DE DESPESA: 44.90.52 e 44.90.40. FONTE DE RECURSOS:**
I M P O R T A N T E **PEDIDOS DE ESCLARECIMENTO ATÉ: ___/___/_____.** **PEDIDOS DE IMPUGNAÇÃO ATÉ: ___/___/_____.** **RECEBIMENTO DAS PROPOSTAS ATÉ: ___/___/_____.** **ABERTURA DAS PROPOSTAS ÀS: __:__ horas do ___/___/_____.** **INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS ÀS: __:__ horas do dia ___/___/_____.**

PROCESSO Nº 00050-00010540/2022-39

O Distrito Federal, representado pela Secretaria de Estado de Segurança Pública do Distrito Federal - SSPDF, torna público, para conhecimento dos interessados, que realizará licitação na modalidade **PREGÃO ELETRÔNICO** do tipo **MENOR PREÇO**, para a aquisição do objeto especificado no Anexo I deste Edital.

O presente certame será regido pela Lei nº 10.520/2002, pelo Decreto Federal nº 10.024/2019, recepcionado no DF pelo Decreto distrital nº 40.205/2019, pelas Leis do DF nº 4.611/2011 e 6.112/2018 (obrigatoriedade da implantação do Programa de Integridade nas empresas que contratarem com o DF), pela Lei complementar nº 123/2006, pelos Decretos distritais nº 36.520/2015, subsidiariamente, 35.592/2014 e 26.851/2006 e alterações posteriores, e, subsidiariamente, pela Lei nº 8.666/1993, **além das demais normas pertinentes**, observadas as condições estabelecidas neste Ato Convocatório e seus Anexos.

O Pregão Eletrônico será realizado em sessão pública, por meio de sistema eletrônico que promova a comunicação pela INTERNET, mediante condições de segurança, utilizando-se, para tanto, os recursos de criptografia e autenticação em todas as suas fases.

Os trabalhos serão conduzidos por servidor designado pela Portaria nº 24/2023, publicada no DODF nº 33, página 49, de 15 de fevereiro de 2023, denominado Pregoeiro, mediante a inserção e monitoramento de dados gerados ou transferidos para a página eletrônica ***https://www.gov.br/compras/pt-br/***, que terá, dentre outras, as seguintes atribuições: receber, examinar e decidir as impugnações e pedidos de esclarecimento ao Edital, apoiado pelo setor responsável pela sua elaboração; conduzir a sessão pública na internet; verificar a conformidade da proposta com os requisitos estabelecidos no instrumento convocatório; dirigir a etapa de lances; verificar e julgar as condições de habilitação; sanear erros ou falhas que não alterem a substância das propostas, dos documentos de habilitação e sua validade jurídica; receber, examinar e decidir os recursos, encaminhando à autoridade competente quando mantiver sua decisão; indicar o vencedor do certame; adjudicar o objeto, quando não houver recurso; conduzir os trabalhos da equipe de apoio; e encaminhar o processo devidamente instruído à autoridade superior e propor sua homologação.

O presente Certame obedecerá as regras estabelecidas no Decreto nº 7.174, de 12/05/2010, recepcionado no Distrito Federal pelo Decreto nº 37.667/2016, que estabelece margem de preferência para bens e serviços com tecnologia desenvolvida no Brasil.

O Edital estará disponível gratuitamente na página **www.ssp.df.gov.br/licitacoes** e no endereço eletrônico ***https://www.gov.br/compras/pt-br/***.

1. DO OBJETO

1.1. Contratação de empresa especializada para fornecer solução de segurança compota por Firewall, do tipo NGFW, de alta capacidade para Segurança de datacenter, firewalls de pequeno porte, gerência centralizada de logs e eventos dos firewall e antivírus com EDR com instalação, configuração, suporte técnico, manutenção e garantia de 36 (trinta e seis) meses, conforme especificações, quantitativos e condições estabelecidas no Termo de Referência e seus anexos.

1.2. A(s) aquisição(ões) visa(m) o atendimento de demanda(s) do(s) seguinte(s) setor(es): Subsecretaria de Modernização Tecnológica.

2. DA DESPESA E DOS RECURSOS ORÇAMENTÁRIOS

2.1. O valor estimado da licitação e os valores unitários e globais dos itens serão tornados públicos após o encerramento da fase de lances.

3. DA DISPONIBILIZAÇÃO DO EDITAL

3.1. Os documentos que integram o Edital serão disponibilizados no portal ComprasGovernamentais (***https://www.gov.br/compras/pt-br/***) e na página da SSPDF (***www.ssp.df.gov.br/licitacoes***), podendo igualmente ser obtidos diretamente na Coordenação de Planejamento, Licitações e Compras Diretas, localizada no Setor de Administração Municipal - SAM Quadra “A” Bloco “A”, CEP 70620-000, Brasília - DF, **somente em mídia digital**, de 2ª a 6ª feira (dias úteis), das 08h00min às 18h00min mediante requerimento da Licitante interessada ao Coordenador de Planejamento, Licitações e Compras Diretas, assinada pelo seu representante legal, devendo fornecer CD/DVD ou levar pen-drive.

4. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

4.1. A **impugnação ao presente Edital e seus anexos** deverá ser dirigida ao Pregoeiro, **até 3 (três) dias úteis** anteriores à data fixada para a abertura da sessão pública, mediante petição a ser enviada exclusivamente por meio eletrônico, através do e-mail **licitacoes@ssp.df.gov.br.**

4.1.1. A impugnação deve estar devidamente identificada (CNPJ, razão social, nome do representante legal e comprovação de poderes para representar a impugnante, se pessoa jurídica, e nome completo e CPF, se pessoa física).

4.1.2. Apresentada a impugnação, caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração do Edital e seus anexos, decidir sobre a impugnação no prazo de 2 (dois) dias úteis, contados da data de recebimento da impugnação.

4.1.3. A impugnação não possui efeito suspensivo, podendo ser concedido o efeito suspensivo por ato do Pregoeiro, devidamente motivado nos autos do processo.

4.1.4. Acolhida a impugnação contra o ato convocatório, será definida e publicada nova data para realização do certame.

4.1.5. A impugnação feita tempestivamente pela Licitante não a impedirá de participar do processo licitatório até o trânsito em julgado da decisão a ela pertinente, devendo, por conseguinte, enviar sua PROPOSTA, até a data e hora marcadas para a abertura da sessão.

4.2. Os **esclarecimentos de dúvidas quanto ao Edital e seus anexos** deverão ser enviados ao Pregoeiro, **até 3 (três) dias úteis** anteriores à data fixada para abertura da sessão pública, mediante petição a ser enviada exclusivamente por meio eletrônico, através do e-mail **licitacoes@ssp.df.gov.br.**

4.2.1. Os pedidos de esclarecimentos deverão estar devidamente identificados (CNPJ, razão social, nome do representante legal e comprovação de poderes para representar a peticionante, se pessoa jurídica, e nome completo e CPF, se pessoa física).

4.2.2. Apresentado pedido de esclarecimento, o Pregoeiro, auxiliado pela unidade requisitante, decidirá sobre a petição, no prazo de até 2 (dois) dias úteis.

4.2.3. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a Administração.

4.3. As impugnações e esclarecimentos serão prestados pelo Pregoeiro diretamente aos peticionantes e serão divulgados a todos os interessados através do site **ComprasGovernamentais** (***https://www.gov.br/compras/pt-br/*** – no *link* correspondente a este Edital), e do site da SSPDF (***www.ssp.df.gov.br/licitacoes***) antes da abertura da sessão, ficando todos os Licitantes obrigados a acessá-los para obtenção das informações prestadas.

4.4. Modificações no Edital serão divulgadas pelo mesmo instrumento de publicação utilizado para divulgação do texto original e o prazo inicialmente estabelecido será reaberto, exceto se, inquestionavelmente, a alteração não afetar a formulação das propostas, resguardado o tratamento isonômico aos Licitantes.

5. DO CREDENCIAMENTO

5.1. O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema **Comprasnet**, provido pela Secretaria de Logística e Tecnologia da Informação – SLTI - ME, por meio do sítio eletrônico ***https://www.gov.br/compras/pt-br/***.

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

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

5.3. O uso da senha de acesso pelo Licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou à SSPDF, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

5.4. A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso.

6. DAS CONDIÇÕES DE PARTICIPAÇÃO NO CERTAME

6.1. Poderão participar deste Pregão as empresas interessadas do ramo de atividade do objeto desta licitação que comprovem sua qualificação, na forma indicada neste Edital:

6.1.1. Que estejam devidamente credenciadas no sistema **Comprasnet**, no endereço eletrônico ***https://www.gov.br/compras/pt-br/***, munidas de chave de identificação e de senha;

6.1.2. Que estejam cadastradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF, nos termos do § 1º, art. 1º do Decreto nº 3.722, de 9 de janeiro de 2001, publicado no D.O.U. de 10 de janeiro de 2001 e art. 4º do Decreto Distrital nº 23.546/03; ou

6.1.3. Que estejam cadastradas no SICAF, mas com seus cadastramentos vencidos, desde que atendidas as exigências do **item 14**, deste Edital.

6.2. NÃO PODERÃO CONCORRER, DIRETA OU INDIRETAMENTE, NESTA LICITAÇÃO OU PARTICIPAR DO CONTRATO DELA DECORRENTE:

6.2.1. Servidor ou dirigente da SSPDF;

6.2.1.1**.** A vedação se aplica para as condições de proprietário, controlador, administrador, gerente ou diretor de pessoa jurídica independentemente das denominações adotadas e do nível quantitativo ou qualitativo de participação no capital ou patrimônio. (§ 1º do Art. 1º do Decreto nº 39.860/2019).

6.2.1.2**.** Aplica-se, ainda, aos executores de contratos que trabalhem ou tenham trabalhado nos últimos cinco anos como sócios, administradores ou não, ou responsáveis pelas entidades contratada, e ao agente público que, na condição referida, esteja licenciado ou afastado por qualquer motivo e a qualquer título.

6.2.1.3. A vedação aplica-se ao agente público licenciado ou afastado por qualquer motivo e a qualquer título.

6.2.1.4. Considera-se participação indireta, para fins do disposto, a existência de qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista entre o autor do projeto, pessoa física ou jurídica, e o licitante ou responsável pelos serviços, fornecimentos e obras, incluindo-se os fornecimentos de bens e serviços a estes necessários.

6.2.2 O autor do termo de referência, do projeto básico ou executivo, pessoa física ou jurídica;

6.2.3 As empresas:

6.2.3.1. Declaradas inidôneas por órgão ou entidade da Administração Pública direta ou indireta, federal, estadual, municipal ou do Distrito Federal;

6.2.3.2. Suspensas de participar de licitação, e impedidas de contratar com a Administração do Distrito Federal, durante o prazo da sanção aplicada;

6.2.3.3. Estrangeiras não autorizadas a funcionar no País;

6.2.3.4. Que se encontrem em processo de dissolução, liquidação, recuperação judicial, recuperação extrajudicial, falência, fusão, cisão ou incorporação;

6.2.3.4.1. Só será permitida a participação de empresas em recuperação judicial e extrajudicial se comprovada, respectivamente, a aprovação ou a homologação do plano de recuperação pelo juízo competente e apresentada certidão emitida pelo juízo da recuperação, que ateste a aptidão econômica e financeira para o certame.

6.2.3.5. Submissas a concurso de credores;

6.2.3.6. Que estejam incluídas no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa disponível no Portal do CNJ;

6.2.3.7. Que conste da relação de inidôneos disponibilizada pelo Tribunal de Contas da União (TCU);

6.2.3.8. Cujo estatuto ou contrato social não incluam o objeto deste Edital;

6.2.3.9. Constituídas com o mesmo objeto e por qualquer um dos sócios e/ou administradores de empresas declaradas inidôneas, após a aplicação dessa sanção e no prazo de sua vigência, observando o contraditório e a ampla defesa a todos os interessados;

6.2.3.10. Isoladamente ou em consórcio, responsável pela elaboração do termo de referência, ou do projeto básico ou executivo, 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;

6.2.3.11. Cujo dirigente, administrador, proprietário ou sócio com poder de direção seja cônjuge, companheiro ou parente, em linha reta ou colateral, por consanguinidade ou afinidade, até o segundo grau, de:

a) Agente público com cargo em comissão ou função de confiança que esteja lotado na unidade responsável pela realização da seleção ou licitação promovida pelo órgão ou entidade da Administração pública distrital; ou;

b) Agente público cuja posição no órgão ou entidade da Administração pública distrital seja hierarquicamente superior ao chefe da unidade responsável pela realização da seleção ou licitação;

6.2.3.11.1. A vedação se aplica aos contratos pertinentes a obras, serviços e aquisição de bens, inclusive de serviços terceirizados, às parcerias com organizações da sociedade civil e à celebração de instrumentos de ajuste congêneres.

6.2.3.11.2. As vedações deste item estendem-se às relações homoafetivas.

6.2.3.12. Reunidas em consórcio, qualquer que seja a sua forma de constituição.

6.3. A participação na presente licitação implica a aceitação plena e irrevogável de todos os termos, cláusulas e condições constantes deste Edital e de seus Anexos, bem como a observância dos preceitos legais e regulamentares em vigor e a responsabilidade pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase do processo.

6.4. As pessoas jurídicas que tenham sócios em comum não poderão participar do certame para o(s) mesmo(s) item(ns).

6.5. Não poderá se beneficiar do tratamento jurídico diferenciado previsto na Lei Complementar nº 123/2006, incluído o regime de que trata o art. 12 da citada Lei Complementar, para nenhum efeito legal, a pessoa jurídica (parágrafo único do art. 2º da Lei nº 4.611/2011):

6.5.1. De cujo capital participe outra pessoa jurídica;

6.5.2 Que seja filial, sucursal, agência ou representação, no País, de pessoa jurídica com sede no exterior;

6.5.3. De cujo capital participe pessoa física que seja inscrita como empresário, ou seja, sócia de outra empresa que receba tratamento jurídico diferenciado nos termos da Lei Complementar nº 123/2006, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do caput do art. 3º da Lei Complementar nº 123/2006;

6.5.4. Cujo titular ou sócio participe com mais de 10% (dez por cento) do capital de outra empresa não beneficiada pela Lei Complementar nº 123/2006, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do caput do art. 3º da Lei Complementar nº 123/2006;

6.5.5. Cujo sócio ou titular seja administrador ou equiparado de outra pessoa jurídica com fins lucrativos, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do caput do art. 3º da Lei Complementar nº 123/2006;

6.5.6. Constituída sob a forma de cooperativas, salvo as de consumo;

6.5.7. Que participe do capital de outra pessoa jurídica;

6.5.8. Que exerça atividade de banco comercial, de investimentos e de desenvolvimento, de caixa econômica, de sociedade de crédito, financiamento e investimento ou de crédito imobiliário, de corretora ou de distribuidora de títulos, valores mobiliários e câmbio, de empresa de arrendamento mercantil, de seguros privados e de capitalização ou de previdência complementar;

6.5.9. Resultante ou remanescente de cisão ou qualquer outra forma de desmembramento de pessoa jurídica que tenha ocorrido em um dos 5 (cinco) anos-calendário anteriores;

6.5.10. Constituída sob a forma de sociedade por ações.

7. DA COTA RESERVADA PARA ENTIDADES PREFERENCIAIS

7.1. Tendo em vista a necessidade de compatibilização e uniformidade dos itens que compõem a presente licitação, não haverá cota reservada para as entidades preferenciais e nem subcontratação compulsória, prevista no art. 48, incisos II e III da Lei Complementar nº 123/2006 e no art. 2º, III, do Decreto-DF nº 35.592/2014.

8. DO ENVIO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

8.1. Após a divulgação do Edital os Licitantes deverão encaminhar a **PROPOSTA INICIAL e os DOCUMENTOS DE HABILITAÇÃO** no endereço eletrônico ***https://www.gov.br/compras/pt-br/***, consignando o **valor global**, bem como a descrição do objeto ofertado.

8.2. As propostas e os documentos de habilitação serão recebidos exclusivamente por meio do sistema eletrônico **Comprasnet** (***https://www.gov.br/compras/pt-br/***), até a data e hora marcadas para a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas e de documentos.

8.3. No momento do envio da proposta e dos documentos de habilitação o Licitante deverá **declarar por meio do sistema eletrônico em campo específico:**

8.3.1. Que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do Edital;

8.3.2. De que até a presente data inexistem fatos impeditivos para a habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores;

8.3.3. 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;

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

8.3.5. Que a proposta apresentada para esta licitação foi elaborada de maneira independente, de acordo com o que é estabelecido na Instrução Normativa nº 2, de 16 de setembro de 2009, da SLTI/MPOG;

8.3.6. Que cumpre os requisitos estabelecidos no art. 3º da Lei Complementar nº 123/2006, bem como de que está apta a usufruir o tratamento favorecido estabelecido nos arts. 42 a 49 da referida Lei Complementar, no caso das Microempresas – ME e Empresas de Pequeno Porte – EPP e Microempreendedores Individuais;

8.4. A assinalação do campo "não" na Declaração do item **8.3.6** apenas produzirá o efeito de a Licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que seja qualificada como microempresa ou empresa de pequeno porte ou microempreendedores individuais.

8.5. As declarações mencionadas nos subitens anteriores serão conferidas pelo Pregoeiro na fase de habilitação.

8.6. Nos casos de emissão de declaração falsa, a empresa Licitante responderá administrativamente na forma do Decreto Distrital nº 26.851/2006.

8.7. **O PREÇO PROPOSTO SERÁ DE EXCLUSIVA RESPONSABILIDADE DO LICITANTE, NÃO LHE ASSISTINDO O DIREITO DE PLEITEAR QUALQUER ALTERAÇÃO DO MESMO, SOB A ALEGAÇÃO DE ERRO, OMISSÃO OU QUALQUER OUTRO PRETEXTO.**

8.8. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

8.9. Para usufruir dos benefícios concedidos pelo Decreto Federal nº 7.174, de 12 de maio de 2010, recepcionado no âmbito do Distrito Federal pelo Decreto Distrital nº 37.667, de 29 de setembro de 2016, a licitante deverá, no momento do cadastramento da proposta, em campo próprio no sistema, indicar se seus produtos ou serviços preenchem os requisitos do Art. 5º da normativa federal. (§ 4º do Art. 7º do Decreto Federal nº 7.174/2010).

8.9.1 Caso a licitante seja beneficiária, deverá ser enviada a documentação pertinente, apta a comprovar o atendimento de tais requisitos, a ser remetida junto à proposta.

9. DAS CONDIÇÕES PARA A ELABORAÇÃO DA PROPOSTA

9.1. O Licitante deverá enviar sua proposta, no idioma oficial do Brasil, mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

9.1.1. Valor unitário e total para cada item ou grupo de itens (conforme o caso), em moeda corrente nacional;

9.1.2. Marca, modelo e fabricante de cada item ofertado;

9.1.3. Descrição detalhada do objeto indicando, no que for aplicável, o prazo de validade e/ou de garantia, número do registro ou inscrição do bem no órgão competente, quando for o caso;

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

9.3. Os quantitativos previstos no orçamento estimado pela Administração não poderão ser alterados pelo proponente.

9.4. O Licitante será responsável por todas as transações que forem efetuadas em seu nome no Sistema Eletrônico, assumindo como firmes e verdadeiras sua proposta e lances.

9.5. A participação no pregão dar-se-á por meio da digitação da senha privativa do Licitante.

9.6. Ao cadastrar sua proposta no sítio do sistema **Comprasnet** o Licitante deverá fazer a descrição detalhada do objeto. Para o detalhamento deverá ser utilizado o campo **"Descrição detalhada do objeto ofertado"**. Não serão aceitas descrições da proposta do tipo **"conforme Edital"**.

9.7. A Licitante que registrar no campo **"Descrição detalhada do objeto ofertado"** qualquer informação que venha a identificar sua razão social ou nome fantasia terá sua proposta desclassificada antes da disputa de lances.

9.8. A omissão de qualquer despesa necessária ao perfeito cumprimento do objeto deste certame será interpretada como não existente ou já incluída no preço, não podendo o Licitante pleitear acréscimo após a abertura da sessão pública.

10. DA CONDUÇÃO DO CERTAME

10.1. Os trabalhos serão conduzidos pelo Pregoeiro, apoiado pela Equipe de Apoio e por setores técnicos, mediante a inserção e monitoramento de dados gerados ou transferidos no endereço eletrônico ***https://www.gov.br/compras/pt-br/***.

10.2. A operacionalidade do sistema **Comprasnet** é de responsabilidade da SLTI/ME, junto a qual as Licitantes deverão informar-se a respeito do seu funcionamento e regulamento, e receber instruções detalhadas para sua correta utilização.

10.3. A participação na licitação na forma eletrônica dar-se-á por meio da digitação da senha pessoal e intransferível do representante credenciado e subsequente encaminhamento da **PROPOSTA e dos DOCUMENTOS DE HABILITAÇÃO**, exclusivamente por meio do sistema eletrônico, observados data e horário estabelecidos neste Edital.

10.4. Incumbirá ao Licitante acompanhar as operações no Sistema Eletrônico durante a sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo Sistema, Pregoeiro ou de sua desconexão.

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

10.6. Quando a desconexão do sistema eletrônico para o Pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente decorridas 24 (vinte e quatro) horas após a comunicação do fato aos participantes, no sítio eletrônico ***https://www.gov.br/compras/pt-br/***.

10.7. No caso de desconexão, cada Licitante deverá de imediato, sob sua inteira responsabilidade, providenciar sua conexão ao sistema.

A abertura da sessão pública deste Pregão, conduzida pelo Pregoeiro, ocorrerá na data e na hora indicadas no preâmbulo deste Edital, no sítio eletrônico ***https://www.gov.br/compras/pt-br/***.

10.8. Durante a sessão pública, a comunicação entre o Pregoeiro e os Licitantes ocorrerá exclusivamente mediante troca de mensagens, via *chat*, em campo próprio do sistema eletrônico. Não será aceito nenhum outro tipo de contato, como meio telefônico ou e-mail;

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

10.10. Somente os Licitantes com propostas classificadas pelo Pregoeiro participarão da fase de lances.

11. DA ABERTURA DAS PROPOSTAS, DA FORMULAÇÃO DE LANCES E DO DESEMPATE

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

11.2. Aberta a sessão pública, o Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, que contenham vícios insanáveis ou que não apresentem as especificações e exigências mínimas constantes no Termo de Referência (Anexo I ao Edital).

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

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

11.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase competitiva.

11.4. Considerando a pequena quantidade de itens, o modo de disputa será o ABERTO.

11.4.1 No modo de disputa ABERTO, a etapa de envio de lances terá duração de 10 (dez) minutos.

11.4.1.1. Durante a fase competitiva, as Licitantes deverão formular seus lances com um intervalo mínimo de diferença de R$ 50,00 (cinquenta reais), conforme tabela constante do item 13.1 do Termo de Referência.

11.4.1.2. O intervalo mínimo de diferença entre os lances incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

11.4.2. Após o período inicial de 10 (dez) minutos, o período inicial será prorrogado automaticamente pelo sistema eletrônico **Comprasnet** quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

11.4.3. A prorrogação automática da etapa de envio de lances, de que trata o subitem **11.4.2**, será de 2 (dois) minutos;

11.4.3.1. A prorrogação automática ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários.

11.4.3.2. São considerados intermediários os lances iguais ou superiores ao menor já ofertado, mas inferiores ao último lance dado pelo próprio Licitante, quando adotado o **julgamento pelo critério de menor preço**.

11.4.4. Na hipótese de não haver novos lances na forma estabelecida nos subitens **11.4.2, 11.4.3** e **11.4.3.1**, a sessão pública será encerrada automaticamente.

11.4.5. Encerrada a etapa competitiva, o sistema ordenará os lances em ordem de vantajosidade em relação ao **menor preço**.

11.4.6. Encerrada a sessão pública sem prorrogação automática pelo sistema **Comprasnet**, na forma dos subitens **11.4.2, 11.4.3** e **11.4.3.1,** o Pregoeiro poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances, em prol da consecução do melhor preço estimado pela Administração, mediante justificativa.

11.5 Encerrada a fase competitiva, se o melhor lance não tiver sido ofertado por empresa qualificada como ME/EPP, o sistema selecionará todas as MEs / EPPs que se encontrem em situação de empate ficto, observada a ordem de classificação, para a convocação para o desempate.

11.6. Na forma da Lei Distrital nº 4.611/2011 e do Decreto Distrital nº 35.592/2014 (art. 4º, § 3º), consideram-se empatadas as propostas de MEs / EPPs com valor igual ou até 5% superior à de **menor preço**.

11.7. Constatada a existência de empate ficto, proceder-se-á a seguinte fase de desempate:

11.7.1. O sistema convocará a ME/EPP para, no prazo de 5 (cinco) minutos, controlados pelo sistema, encaminhar uma última oferta **obrigatoriamente mais vantajosa** que a proposta da primeira colocada.

11.7.2. Caso a ME/EPP não ofereça proposta mais vantajosa, o sistema convocará os Licitantes ME/EPP remanescentes que porventura se encontrem dentro da margem de preferência, seguindo-se a ordem de classificação, para o exercício do mesmo direito.

11.7.3. Na hipótese de não oferta de lance que desempate o procedimento licitatório, permanecerá a ordem de classificação anteriormente determinada.

11.7.4. O Pregoeiro poderá solicitar documentos que comprovem o enquadramento do Licitante como ME/EPP.

11.8. Após o desempate de que tratam os subitens **11.5** a **11.7**, caso persista o empate entre duas ou mais propostas, será assegurada preferência, sucessivamente, aos bens:

a) Produzidos no País;

b) Produzidos ou prestados por empresas brasileiras;

c) Produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

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

11.8.1. Os critérios de desempate previstos nos subitens **11.5** a **11.8** serão aplicados caso não haja envio de lances após o início da fase competitiva.

11.10 DA APLICABILIDADE DO DECRETO N.º 7.174/2010.

11.10.1 Por força do que dispõe o art. 3º da Lei nº 8.248, de 1991 e do Decreto Distrital nº 34.367/2013, 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.

11.10.1.1 Para usufruir dos benefícios concedidos pelo Decreto Federal nº 7.174/2010, a licitante deverá, no momento do cadastramento da proposta, em campo próprio no sistema, indicar se seus produtos ou serviços preenchem os requisitos do Art. 5º da normativa federal. (§ 4º do Art. 7º do Decreto Federal nº 7.174/2010).

11.10.1.2 Em se tratando de licitação com grupos ou lotes o Sistema não foi adaptado à utilização do Decreto, devendo ser realizado de forma manual, com a entrega de **Declaração** de que possui direito ao benefício de preferência estabelecido no Decreto 34.367/2013 c/c Decreto 7.174/2010, **conforme modelo disposto no anexo VI**.

11.10.1.3 **A ausência da Declaração citada no subitem 11.10.1.2 acarretará a preclusão consumativa do pretenso direito.**

11.10.2 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.

11.10.3 As licitantes que declararam no sistema, quando do cadastro de suas propostas, que atendem aos requisitos estabelecidos no art. 5º do Decreto nº 7.174, de 2010, serão convocadas a exercerem o seu direito de preferência, observada a seguinte ordem de classificação, na forma definida pelo Poder Executivo Federal:

1º - bens com Tecnologia desenvolvida no País e produzido de acordo com o Processo Produtivo Básico (PPB) + Micro e Pequena Empresa;

2º - bens com Tecnologia desenvolvida no País e produzido de acordo com o Processo Produtivo Básico (PPB);

3º - bens com Tecnologia desenvolvida no País + Micro e Pequena Empresa;

4º - bens com Tecnologia desenvolvida no País;

5º - bens produzidos de acordo com o Processo Produtivo Básico (PPB) + Micro e Pequena Empresa;

6º - bens produzidos de acordo com o Processo Produtivo Básico (PPB)

11.10.3.1 Aplicar-se-ão as regras de preferência previstas neste item com a classificação dos licitantes cujas propostas finais estejam situadas até 10% (dez por cento) acima da melhor proposta válida, considerando o valor global, caso se trate de grupo/lote, conforme o critério de julgamento, para a comprovação e o exercício do direito de preferência.

11.10.3.1.1 Serão convocadas as licitantes classificadas que estejam enquadradas nas condições previstas no subitem 3.8.3, 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.

11.10.4 Caso nenhuma empresa classificada venha a exercer o direito de preferência, será declarada vencedora a licitante detentora da proposta originalmente vencedora do certame.

11.10.5 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.

11.10.6 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 10.521, de 2021.

11.10.6.1 A comprovação será feita:

I - 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

II - Por documento expedido para esta finalidade pelo Ministério da Ciência e Tecnologia ou pela SUFRAMA, mediante solicitação da licitante.

11.10.7 A licitante deverá encaminhar juntamente com a proposta, a documentação e 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.

11.10.8 O licitante que optar por usufruir dos benefícios do Decreto nº 7.174/2010 deverá enviar, juntamente com a sua proposta, a auto declaração de que possui direito ao benefício, **conforme modelo disposto no Anexo VI do Edital.**

11.10.9 Até que o Sistema de Compras seja alterado para operar automaticamente as preferências previstas no Decreto em referência, **o Pregoeiro aplicará manualmente os benefícios do Decreto nº 7.174/2010, após a fase de lances e antes da aceitação**, se necessário, com a suspensão da sessão, sendo imprescindível o preenchimento e envio da Declaração, constante no Anexo VI.

11.10.10 Ressaltamos que a verificação do(s) certificado(s) permanece como procedimento de habilitação, portanto, restrita ao licitante de melhor lance.

11.11 Na hipótese de persistir o empate, a proposta vencedora será sorteada pelo sistema **Comprasnet,** dentre as propostas empatadas.

12. DA NEGOCIAÇÃO DIRETA

12.1. Após o encerramento da fase competitiva, o Pregoeiro encaminhará, pelo sistema eletrônico, contraproposta ao Licitante que tenha apresentado lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento.

12.2. É vedada a negociação com condições diferentes das previstas neste Edital.

12.3. A negociação será realizada por meio do sistema, podendo ser acompanhada pelas demais Licitantes.

13. DO JULGAMENTO DA PROPOSTA VENCEDORA

13.1. Encerrada a etapa competitiva e depois da verificação de possível empate, o Pregoeiro examinará a(s) proposta(s) classificada(s) em primeiro lugar quanto ao **preço** e quanto ao atendimento das especificações.

13.2. O(s) Licitante(s) classificado(s) em primeiro lugar, após a negociação, deverá(ão) enviar **no prazo de 02 (duas) horas** a contar da requisição do Pregoeiro via chat, a(s) Proposta(s) de Preços devidamente atualizada(s), em conformidade com o valor negociado ou o último lance ofertado.

13.3. A proposta ajustada será recebida **exclusivamente por meio do sistema Comprasnet** (opção "Enviar Anexo"), respeitado o limite do sistema eletrônico, podendo ser incluídos quantos arquivos forem necessários.

13.4. A(s) proposta(s) atualizada(s) deverá(ão) ser lavrada(s) em língua portuguesa e deve(m) conter:

13.4.1. Nome da proponente e de seu representante legal, endereço completo, telefone, endereço de correio eletrônico, números do CNPJ e da inscrição Estadual, Municipal e Distrital;

13.4.2. Preço unitário e total de cada objeto cotado, devendo estar inclusas nos preços ofertados todas as despesas que incidam ou venham a incidir sobre o objeto;

13.4.3. A indicação de uma única marca e modelo para cada objeto, sem prejuízo da indicação de todas as características do produto cotado, com especificações claras e detalhado, inclusive tipo, referência, número do registro ou inscrição do bem no órgão competente quando for o caso, observadas as especificações constantes no Anexo I deste Edital;

13.4.4. Prazo de validade da proposta, não devendo ser inferior a 90 (noventa) dias corridos, contados da data prevista para abertura da licitação;

13.4.5. Prazo de entrega e instalação dos bens: até 60 (sessenta) dias úteis, contados da assinatura do contrato ou do recebimento da Nota de Empenho, quando não houver a formalização do instrumento contratual;

13.4.6. Declaração expressa, de que nos preços ofertados estão incluídas todas as despesas relativas à entrega do(s) bem(ns) tais como embalagens, encargos sociais, frete, seguro, tributos e encargos de qualquer natureza que, direta ou indiretamente, incidam sobre o objeto da licitação;

13.4.7. Declaração de que a Licitante atende os critérios de sustentabilidade ambiental previstos no atr. 7º da Lei Distrital nº 4.770/2012, conforme modelo constante no **Anexo III**. A declaração pode ser substituída por certificação emitida por instituição pública oficial ou instituição credenciada, ou qualquer outro meio de prova, que ateste que a empresa cumpre com as exigências de práticas de sustentabilidade ambiental;

13.4.8. Memórias de Cálculo que, eventualmente, se fizerem necessárias; e

13.5. Os dados inseridos na proposta, como correio eletrônico, número de telefone e fax, serão utilizados para a comunicação oficial entre a SSPDF e a empresa, tanto na fase licitatória quanto na fase contratual.

13.6. Em nenhuma hipótese, o conteúdo das propostas poderá ser alterado, seja com relação às características técnicas, marcas, modelos, prazo de entrega, prazo de garantia e preço dos equipamentos e materiais ou de qualquer outra condição que importe modificação dos seus termos originais, **ressalvadas as hipóteses destinadas a sanar apenas falhas formais, alterações essas que serão analisadas pelo Pregoeiro**.

13.7. Serão corrigidos automaticamente pelo Pregoeiro quaisquer erros aritméticos, bem como as divergências que porventura ocorrerem entre o preço unitário e o total do item, quando prevalecerá sempre o primeiro.

13.8. Em consonância com o § 3º, art. 43, da Lei nº 8.666/1993, para fins de verificação/comprovação quanto ao atendimento das especificações contidas no Termo de Referência, o Pregoeiro poderá promover diligência destinada a esclarecer ou a complementar a instrução do processo, requerendo a remessa de folders, catálogos, prospectos técnicos, dentre outros que julgar cabíveis à análise objetiva dos produtos ofertados pelas Licitantes.

13.9. O Pregoeiro poderá, se necessário, suspender a sessão para recorrer a setores técnicos internos e externos, bem como aos órgãos requisitantes da compra do material objeto deste Pregão, a fim de obter parecer que possibilite melhor julgamento das especificações dos produtos cotados, definindo nova data para continuidade da sessão licitatória.

13.10. Não serão aceitas propostas que apresentarem preços globais ou unitários simbólicos, irrisórios ou de valor zero, bem como propostas que apresentarem valores globais e unitários acima do estimado.

13.11. Serão desclassificadas propostas que contenham preços excessivos ou manifestamente inexequíveis, assim entendidos:

13.11.1. Preços excessivos, quando os mesmos apresentarem valores superiores ao preço estimado pela Administração;

13.11.1.1. A desclassificação por preços excessivos somente ocorrerá após a fase competitiva, caso a Administração não obtenha êxito na negociação direta.

13.11.2. Preços inexequíveis, quando os mesmos forem inferiores ao custo de produção, acrescidos dos encargos legais;

13.11.2.1. O Licitante será convocado para demonstrar a exequibilidade do preço ofertado, e, caso não demonstre, será desclassificado.

13.12. **Serão analisados, para a definição de valores excessivos ou inexequíveis, os preços unitários e globais.**

13.13. O não envio da proposta ajustada por meio do sistema **Comprasnet** (opção "Enviar Anexo"), com todos os requisitos ou o descumprimento das eventuais diligências determinadas pelo Pregoeiro acarretará na desclassificação da proposta.

13.14. Sempre que a proposta não for aceita, antes de ocorrer a convocação da Licitante subsequente, haverá nova verificação da eventual ocorrência do empate ficto, previsto nos subitens **11.5** a **11.7**, visto o disposto na Lei Distrital nº 4.611/2011 e no Decreto Distrital nº 35.592/2014.

13.15. Em caráter de diligência, os documentos remetidos por meio da opção "Enviar Anexo" do sistema **Comprasnet** poderão ser solicitados em original ou por cópia autenticada, a qualquer momento. Nesse caso, os documentos deverão ser encaminhados, no prazo estabelecido pelo Pregoeiro, para a Coordenador de Planejamento, Licitações e Compras Diretas, sito ao Setor de Administração Municipal - SAM Quadra "A" Bloco "A", CEP 70620-000, Brasília - DF.

14. DA HABILITAÇÃO

14.1. Encerrada a fase de propostas, o Pregoeiro promoverá a análise dos documentos de habilitação enviados pelo Licitante, conforme regulado neste Edital.

14.2. Em caráter de diligência, os documentos de habilitação remetidos por meio da opção "Enviar Anexo" do sistema **Comprasnet** poderão ser solicitados em original ou por cópia autenticada, a qualquer momento. Nesse caso, os documentos deverão ser encaminhados, no prazo estabelecido pelo Pregoeiro, para a Coordenador de Planejamento, Licitações e Compras Diretas, sito ao Setor de Administração Municipal - SAM Quadra "A" Bloco "A", CEP 70620-000, Brasília - DF.

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

14.4. Constatada a existência de sanção, o Pregoeiro inabilitará o Licitante, por falta de condição de participação.

14.5. Realizadas as diligências, o Pregoeiro fará a análise dos documentos de habilitação.

14.6. DOS LICITANTES CADASTRADOS NO SICAF:

14.6.1. As Licitantes devidamente cadastradas no SICAF deverão encaminhar os seguintes documentos:

14.6.2. Documentação relativa à habilitação técnica elencada nos subitens **14.10.1**, **14.10.2** deste Edital. Caso o SICAF apresente parte dos documentos de qualificação técnica, deverão ser apresentados os documentos faltantes;

14.6.3. Certidão Negativa de falência, recuperação judicial ou extrajudicial (Lei nº 11.101, de 09/02/2005), expedida pelo distribuidor da sede da empresa, **datado dos últimos 90 (noventa) 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;

14.6.4. Os Licitantes que apresentarem resultado menor ou igual a 1 (um), em qualquer um dos índices contidos no cadastro do SICAF, deverão comprovar capital social ou patrimônio líquido mínimo de 10% (dez por cento) do valor total estimado para o(s) item(ns) cotado(s) constante do Anexo I, **a ser divulgado após a fase de lances, que deverá recair sobre o montante dos itens que pretenda concorrer**;

14.6.5. A comprovação deverá ser feita quando da habilitação, apresentando o balanço Patrimonial e Demonstrações Contábeis do último exercício social, já exigíveis e apresentados na forma da Lei, devidamente registrados ou pelo registro comercial, ato constitutivo, estatuto ou contrato social;

14.6.6. Declarações prestadas diretamente no sistema, na forma do **item 8.3** deste Edital;

14.6.7. Todas as declarações constantes do sistema ComprasGovernamentais serão consultadas e juntadas aos autos do processo.

14.6.8. Prova de regularidade com a Secretaria de Estado de Economia do Distrito Federal, que poderá ser obtida por meio do site www.fazenda.df.gov.br **(também é obrigatória para os Licitantes com sede ou domicílio fora do Distrito Federal**).

14.6.9. A Licitante cuja habilitação parcial no SICAF acusar no demonstrativo "Consulta Situação do Fornecedor", algum documento com validade vencida, deverá encaminhar o respectivo documento a fim de comprovar a sua regularidade.

14.6.10. Os Licitantes que estiverem cadastrados no Sistema de Cadastro Unificado de Fornecedores – SICAF vencidos, deverão apresentar a seguinte documentação relativa à Habilitação Jurídica, à Regularidade Fiscal e trabalhista, Habilitação Econômico-Financeira e Qualificação Técnica:

14.7. COMPROVAÇÃO DA HABILITAÇÃO JURÍDICA:

14.7.1. Documento de identificação contendo todos os dados dos responsáveis legais da proponente;

14.7.2. Registro comercial, arquivado na Junta Comercial respectiva, no caso de empresa individual;

14.7.3. 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;

14.7.4. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;

14.7.5. 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.

14.7.6. Procuração por instrumento público, ou por instrumento particular com o devido reconhecimento de firma em cartório, comprovando a delegação de poderes para assinatura e rubrica dos documentos integrantes da habilitação e propostas, quando estas não forem assinadas por diretor(es), com poderes estatutários para firmar compromisso.

14.8. REGULARIDADE FISCAL E TRABALHISTA:

14.8.1. Registro no Cadastro Nacional de Pessoa Jurídica – CNPJ;

14.8.2. Prova de inscrição no cadastro de contribuinte Estadual, Municipal ou do Distrito Federal, se houver, relativo ao domicilio ou sede do Licitante, pertinente ao ramo de atividade e compatível com o objeto contratual;

14.8.3. Prova de regularidade com as Fazendas Estadual e Municipal, do domicílio ou sede da Licitante;

14.8.4. Prova de regularidade com a Secretaria de Estado de Economia do Distrito Federal, **independentemente da sede ou domicílio do Licitante**, que poderá ser obtida por meio do site ***www.fazenda.df.gov.br***;

14.8.5. Prova de Regularidade junto à **Fazenda Nacional** (Débitos e Tributos Federais), à **Dívida Ativa da União** e junto à **Seguridade Social** (contribuições sociais previstas nas alíneas "a" a "d" do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991 – contribuições previdenciárias e as de terceiros), fornecida por meio da Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União;

14.8.6. Certificado de Regularidade perante o FGTS, fornecido pela Caixa Econômica Federal, devidamente atualizado, nos termos da Lei nº 8.036, de 11.5.90;

14.8.7. Certidão de regularidade relativa a débitos inadimplidos perante a Justiça do Trabalho (CNDT), mediante a apresentação de certidão negativa, em plena validade, que poderá ser obtida no site ***www.tst.jus.br/certidao***.

14.8.8. Para todas as certidões referentes à regularidade fiscal e trabalhista, serão aceitas certidões positivas com efeitos de negativa.

14.8.9. Caso o Licitante seja considerado isento de tributos estaduais ou municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Estadual ou da Fazenda Municipal do domicílio ou sede do fornecedor, ou outra equivalente, na forma da lei.

14.9. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA:

14.9.1. Certidão Negativa de falência, de recuperação judicial ou extrajudicial (Lei nº 11.101, de 09/02/2005), expedida pelo distribuidor da sede da empresa, **datado dos últimos 90 (noventa) 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;

14.9.2. 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.

14.9.3. As empresas constituídas no ano em curso poderão substituir o balanço anual por balanço de abertura, devidamente autenticado pela Junta Comercial;

14.9.4. A boa situação financeira da empresa será avaliada pelos Índices de Liquidez Geral (LG) e Liquidez Corrente (LC) e Solvência Geral (SG), resultantes da aplicação das seguintes fórmulas:

1. **ILG: Índice de Liquidez Geral ≥ 1 (maior ou igual a 1)**

$$\textbf{ILG} = \frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}} > 1$$

2. **ILC: Índice de Liquidez Corrente ≥ 1 (maior ou igual a 1)**

$$\textbf{ILC} = \frac{\text{ATIVO CIRCULANTE}}{\text{PASSIVO CIRCULANTE}} > 1$$

3. **SG: Solvência Geral ≥ 1 (maior ou igual a 1)**

$$\textbf{SG} = \frac{\text{ATIVO TOTAL}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}} > 1$$

14.9.5. O balanço patrimonial e as demonstrações contábeis deverão estar assinados por Contador ou por outro profissional equivalente, devidamente registrado no Conselho Regional de Contabilidade.

14.9.5.1. Serão consideradas como detentoras de capacidade econômico-financeira satisfatória as Licitantes que obedecerem simultaneamente às condições do item**14.9.4.** (1, 2 e 3) acima.

14.9.5.2. A Licitante deverá apresentar os cálculos constantes do item **14.9.4**, assinados por seu representante legal e por um contador.

14.9.5.3. As empresas que apresentarem resultado inferior ao mínimo estabelecido em qualquer dos índices referidos no item b.2, quando de suas habilitações, deverão comprovar, considerados os riscos para a Administração, através do Balaço Patrimonial do exercício social já exigível e devidamente registrado na Junta Comercial, Patrimônio Líquido ou Capital Social mínimo de 10% (dez por cento) do valor estimado para a contratação do(s) item(ns) cotado(s) constante do Anexo I, **a ser divulgado após a fase de lances, que deverá recair sobre o montante dos itens que pretenda concorrer**. A comprovação deverá ser feita relativamente à data da apresentação da proposta, admitida a atualização para esta data através de índices oficiais.

14.10. QUALIFICAÇÃO TÉCNICA:

14.10.1. Comprovação de aptidão no desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação – **ATESTADO(S) DE CAPACIDADE TÉCNICA**, em língua portuguesa do Brasil, fornecido(s) por pessoa jurídica de direito público ou privado, onde deverá indicar dados da entidade emissora e dos signatários do documento, além da descrição do objeto e quantidades, comprovando ter a Licitante fornecido materiais/equipamentos compatíveis com o objeto desta licitação, considerando-se compatível o fornecimento anterior de objeto com as seguintes características:

14.10.1.1 As empresas licitantes deverão apresentar comprovação de aptidão no desempenho de atividade pertinente, para os GRUPOS 1 e 2, compatível em características com os objetos desta licitação, por intermédio da apresentação de Atestado(s) de Capacidade Técnica, fornecido(s) por pessoa jurídica de direito público ou privado.

14.10.1.2 Considera(m)-se compatível(eis) o(s) atestado(s) que expressamente certifique(m) que o proponente já prestou serviços pelo menos 50% (cinquenta por cento) do quantitativo a ser contratado, estabelecido neste Termo de Referência, de acordo com o TCU, Acórdãos de Plenário nº 1.284/2003, nº 2.068/2004, nº 2.088/2004, nº 2.656/2007, nº 2.056/2008 e nº 11.213/2013.

14.10.2. Será permitido a soma de atestado (s), visando comprovar o quantitativo estabelecido acima;

14.11. DA HABILITAÇÃO DAS MEs / EPPs:

14.11.1. As empresas qualificadas como MEs / EPPs, na forma da Lei Complementar nº 123/2006, deverão apresentar **todos os documentos de habilitação**, referentes à habilitação jurídica, fiscal, econômico-financeira e técnica, sob pena de inabilitação.

14.11.2. A existência de restrição relativamente à **regularidade fiscal e trabalhista** não impede que a Licitante qualificada como microempresa (ME) ou empresa de pequeno porte (EPP) ou microempreendedores individuais seja declarada vencedora, uma vez que atenda a todas as demais exigências do Edital.

14.11.3. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

14.11.4. Caso a proposta mais vantajosa seja ofertada por Licitante qualificada como microempresa ou empresa de pequeno porte ou microempreendedores individuais, e uma vez constatada a existência de alguma restrição no que tange à **regularidade fiscal e trabalhista**, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização.

14.11.5. O prazo poderá ser prorrogado por igual período, a critério da Administração, quando requerida pelo Licitante, mediante apresentação de justificativa.

14.11.6. A não regularização no prazo previsto implicará decadência do direito à contratação, sem prejuízo das sanções previstas neste Edital, sendo facultada à SSPDF convocar os Licitantes remanescentes, na ordem de classificação para prosseguimento do certame, ou revogar a licitação.

14.11.7. O tratamento favorecido e diferenciado não poderá ser aplicado em favor de entidade que, em decorrência do valor dos itens da licitação a que estiver concorrendo, venha a auferir faturamento que acarrete o seu desenquadramento da condição de microempresa, conforme dispõe o art. 24 da Lei distrital nº 4.611/2011 e art. 2º, § 2º, do Decreto distrital nº 35.592/2014.

14.12. OBSERVAÇÕES GERAIS SOBRE A HABILITAÇÃO:

14.12.1. Os documentos apresentados para habilitação deverão estar todos **em nome e CNPJ da matriz** ou todos **em nome e CNPJ da filial**, exceto aqueles que comprovadamente só possam ser fornecidos à matriz e referir-se ao local do domicílio ou sede do interessado.

14.12.2. As certidões que não apresentarem em seu teor, data de validade previamente estabelecida pelo Órgão expedidor, **deverão estar datadas dos últimos 90 (noventa) dias**, contados da data da sessão pública deste Pregão.

14.12.3. Será inabilitado o Licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

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.

14.12.4. Caso de inabilitação, haverá nova verificação da eventual ocorrência do empate ficto, previsto nos subitens **11.5** a **11.7**, visto o disposto na Lei Distrital nº 4.611/2011 e no Decreto Distrital nº 35.592/2014.

14.12.5. Constatado o atendimento pleno às exigências fixadas neste Edital, a Licitante será declarada vencedora.

14.12.6. O Pregoeiro diligenciará na internet para evitar inabilitações pela falta de apresentação de documentos de regularidade fiscal, jurídica, econômico-financeira e técnica, visando a manutenção da proposta de melhor preço.

15. DOS RECURSOS

15.1. Declarado o vencedor, qualquer Licitante poderá, durante o prazo concedido na sessão pública, de forma imediata, em campo próprio do sistema **Comprasnet**, manifestar sua intenção de recorrer.

15.2. A ausência de manifestação imediata e motivada do Licitante quanto à intenção de recorrer, nos termos do disposto no subitem **15.1** importará na decadência desse direito.

15.3. As manifestações de intenção de recorrer devem ser feitas exclusivamente por meio do sistema **Comprasnet**.

15.4. As manifestações fora do sistema **Comprasnet** serão desconsideradas.

15.5. Nesse momento o Pregoeiro não adentrará no mérito recursal, verificando somente as condições de admissibilidade do recurso.

15.6. A ausência de manifestação ou as manifestações fora do sistema acarretarão no prosseguimento do feito, estando o Pregoeiro autorizado a adjudicar o objeto ao Licitante declarado vencedor.

15.7. Recebida a intenção de interpor recurso pelo Pregoeiro, a Licitante deverá apresentar as razões do recurso no prazo de 3 (três) dias, ficando as demais Licitantes, desde logo, intimadas para, querendo, apresentar contrarrazões.

15.8. O prazo para apresentação de contrarrazões será de 3 (três) dias e começará imediatamente após o encerramento do prazo recursal.

15.9. As razões e contrarrazões serão recebidas somente no portal **Comprasnet**, por meio de campo próprio do sistema. **Não serão recebidas e conhecidas razões de recurso e contrarrazões enviadas diretamente ao Pregoeiro ou por quaisquer outros meios (fax, correspondência, correio eletrônico, etc)**.

15.10. Os interessados que porventura queiram ter vista do processo licitatório poderão requisitar a disponibilização de acesso externo ao inteiro teor do processo eletrônico por meio do e-mail: licitacoes@ssp.df.gov.br endereçado ao Subsecretário de Administração Geral.

15.11. Caberá ao Pregoeiro receber, examinar e instruir os recursos impetrados contra seus atos, podendo reconsiderar suas decisões no prazo de 5 (cinco) dias úteis após o recebimento das razões e contrarrazões ou, neste mesmo prazo, fazê-lo subir devidamente relatado ao Subsecretário e Administração Geral da SSPDF para a decisão final no prazo de 5 (cinco) dias úteis, na forma do art. 13, IV, e do art. 45, tudo do Decreto Federal nº 10.024/2019.

15.12. O acolhimento do recurso importará na invalidação apenas dos atos que não podem ser aproveitados.

15.13. O recurso contra decisão do Pregoeiro terá efeito suspensivo.

16. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

16.1. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto e homologará o procedimento licitatório.

16.2. Na ausência de recurso, caberá ao Pregoeiro adjudicar o objeto e encaminhar o processo devidamente instruído à autoridade superior, propondo sua homologação.

16.3. Constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

17. DO CONTRATO

17.1. Após a homologação da licitação, a Licitante vencedora será convocada para assinar o termo de contrato, ou retirar documento equivalente, no prazo de 5 (cinco) dias úteis contados da data do recebimento do Termo de Convocação.

17.2. O convocado poderá, a critério da Administração, assinar o contrato diretamente no processo eletrônico (assinatura eletrônica), cabendo à Administração, mediante prévio cadastro, a liberação para assinatura de usuário externo no SEI.

17.3. O prazo para assinatura do Contrato estabelecido no **item 17.1** poderá ser prorrogado uma única vez, por igual período, quando solicitado pela Licitante vencedora, durante o seu transcurso e desde que ocorra motivo justificado e aceito pelo Subsecretário de Administração Geral da SSPDF.

17.4. Na assinatura do contrato será exigida a comprovação das condições de habilitação consignadas no Edital, que deverão ser mantidas pelo Licitante durante toda a vigência contratual.

17.5. O Contrato a ser assinado subordina-se ao Termo Padrão nº **07/2002**, em conformidade com o Decreto 23.287 de 17/10/2002 do Distrito Federal, que segue como **Anexo IV a este Edital**, e terá **vigência de 36 (trinta e seis) meses**, a contar de sua assinatura.

17.6. A vigência contratual poderá ser prorrogada nas hipóteses previstas no artigo 57 da Lei nº 8.666/93.

17.7. Após a celebração do contrato, a Licitante vencedora deverá, no prazo de até 10 (dez) dias da assinatura do contrato, prorrogável por igual período, prestar uma das seguintes garantias:

17.7.1. 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)

17.7.2. seguro-garantia; ou,

17.7.3. fiança bancária.

17.8. Caberá ao contratado optar por uma das modalidades de garantia acima, no percentual de 2% (dois por cento) do valor do contrato.

17.9. **A garantia deverá ter validade igual ou superior a 90 dias após a vigência do contrato.**

17.10. Caso a Contratada opte pela caução em dinheiro, a empresa deverá realizar TED ou depósito para a Secretaria de Estado de Fazenda do Distrito Federal, CNPJ 00.394.684/0001-53, no Banco Regional de Brasília (BRB) Agência 100; Conta 800482-8.

17.11. Toda e qualquer garantia prestada pela Licitante vencedora:

a) somente poderá ser levantada 90 (noventa) dias após a extinção do contrato, e quando em dinheiro, atualizada monetariamente;

b) poderá, a critério da SSPDF, ser utilizada para cobrir eventuais multas e/ou para cobrir o inadimplemento de obrigações contratuais, sem prejuízo da indenização eventualmente cabível. Nesta hipótese, no prazo máximo de 15 (quinze) dias corridos após o recebimento da notificação regularmente expedida, a garantia deverá ser reconstituída;

c) ficará retida no caso de rescisão contratual, até definitiva solução das pendências administrativas ou judiciais.

17.12. Nos casos de alterações contratuais que promovam acréscimos ao valor inicialmente contratado, a garantia prestada deverá ser reforçada e/ou renovada.

17.13. A garantia prestada deverá ser comprovada junto a Coordenador de Orçamento, Finanças, Fundos, Contratos e Convênios, no prazo previsto no item **17.7**.

17.14. O Contrato poderá ser alterado na ocorrência de quaisquer fatos estipulados no art. 65 da Lei nº 8.666/93 e suas alterações.

17.15. Todo e qualquer pedido de alteração do Contrato oriundo desta licitação deverá ser dirigido ao Executor de Contrato ou ao Presidente da Comissão Executora do Contrato, a quem caberá análise do pedido e encaminhamento ao Subsecretário de Administração Geral da SSPDF a quem caberá o deferimento ou não do pedido.

17.16. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no Edital ou se recusar a assinar o contrato, outro Licitante poderá ser convocado, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato, sem prejuízo da aplicação das sanções de que trata o Decreto Distrital nº 26.851/2006.

17.17. Este Edital, o Termo de Referência e seus anexos e a proposta de preços apresentada pela Licitante vencedora farão parte integrante do Contrato.

17.18. A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais, legais e regulamentares.

17.19. São vedadas a subcontratação total ou parcial acima dos limites estabelecidos neste Edital, a associação da Contratada com outrem, a sub-rogação, cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação.

17.20. Será designado um Executor, ou uma Comissão Executora de Contrato, que terá as atribuições contidas na Lei 8.666/1993 e no Decreto Distrital nº 32.598/2010, a quem caberá a fiscalização e acompanhamento da obra nos termos do Edital, Projeto Básico e seus anexos.

17.21. A Contratada se obriga a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões do valor total inicial atualizado do Contrato que se fizerem necessários, observado o percentual máximo de 25% (vinte e cinco por cento), salvo as supressões resultantes de acordos celebrados entre as partes, na forma do art. 65, §§ 1º e 2º, da Lei nº 8.666/1993.

17.22. Incumbirá à SSPDF providenciar a publicação resumida do instrumento de contrato e de seus eventuais termos aditivos no Diário Oficial do Distrito Federal (DODF).

18. DO REAJUSTE

18.1. Observado o interregno mínimo de um ano a partir da data limite para apresentação da proposta, o Contrato celebrado poderá, à pedido da empresa, ter seu valor anualmente reajustado, pelo Índice Nacional de Preços ao Consumidor Amplo – IPCA (art. 2º do Decreto Distrital nº 37.121, publicado no DODF nº 31, de 17 de fevereiro de 2016), ou aquele que vier a substituí-lo, apurado durante o período.

18.2. O prazo para a CONTRATADA requerer o reajuste contratual estipulado no item acima extinguir-se-á:

18.2.1 com o fim do prazo de vigência, momento em que ocorrerá a preclusão temporal; ou

18.1.2. com a formalização após o interregno mínimo de um ano de Termo Aditivo de alteração quantitativa/qualitativa ou de revisão contratual, momento em que ocorrerá a preclusão consumativa.

18.3. Os efeitos financeiros decorrentes do reajuste contratual vigorarão a partir da data do pedido.

19. DOS ADITAMENTOS CONTRATUAIS

19.1. As alterações das especificações para melhor adequação técnica aos objetivos da contratação, à pedido da SSPDF, **desde que não decorrentes de erros ou omissões por parte da CONTRATADA**, serão processados por meio de termo aditivo, observados os limites previstos no item **17.21** deste Edital (§ 1º do art. 65 da Lei nº 8.666/93).

19.2. As eventuais modificações de tratam o item 19.1, condicionam-se à elaboração de justificativa prévia, devidamente aceita pelo Subsecretário de Administração Geral da SSPDF.

19.3. As alterações de valor contratual, decorrente do reajuste de preços, compensação ou penalização financeira prevista no contrato, bem como o empenho de dotações orçamentárias suplementares, até o limite do respectivo valor contratado, dispensam a celebração de aditamento, podendo ser processadas por meio de apostila.

20. **DA FISCALIZAÇÃO**

20.1. Sujeitar-se-á a Contratada à mais ampla e irrestrita fiscalização da autoridade encarregada de acompanhar a execução do objeto desta licitação, prestando todos os esclarecimentos solicitados e atendendo às exigências formuladas dentro das prescrições legais.

20.2. A fiscalização da Contratante não eximirá, em hipótese alguma, a Contratada de quaisquer outras fiscalizações de órgãos oficiais, quanto às obrigações tributárias, fiscais, trabalhistas e demais que se fizerem necessárias.

20.3. A fiscalização de que trata esta Cláusula não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade resultante de imperfeições técnicas, vícios redibitórios ou emprego de material inadequado ou de qualidade inferior e, na ocorrência deste, não implica corresponsabilidade da Administração Contratante ou de seus agentes e prepostos.

20.4. Quaisquer exigências da fiscalização, inerentes ao objeto do presente Edital, deverão ser prontamente atendidas pela Contratada, sem ônus para a SSPDF.

21. DO RECEBIMENTO DO OBJETO

21.1. O objeto da licitação deverá ser entregue/instalado, no prazo de até 60 dias úteis, conforme cronograma detalhado no Termo de Referência, contados da data de recebimento da Nota de Empenho ou da assinatura do termo contratual. As unidades que receberão os bens são: CIOB - Centro Integrado de Operações de Brasília - SAM - Conjunto A bloco "D" - Edifício anexo da Sede da SSP/DF - CEP 70610-640 - Brasília DF; SUDEC - Defesa Civil - SIA Trecho 06, lote 25-35 Ed. Business Center - CEP 71205-060 - Brasília DF; GETRAM - Gerência de Transporte e Manutenção - SIA Trecho 4 Lote 1480 Edifício SENAP I - CEP 71200-040 - Brasília DF; NUAL - Núcleo de Almoxarifado e NUPAT - Núcleo de Patrimônio, SGO Quadra 5 Lote 795 CEP 70610-650 - Brasília DF.

21.2. A entrega deverá ocorrer em dia de expediente da SSPDF, nos horários compreendidos entre 08h00 às 17h00.

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

21.3.1. PROVISORIAMENTE, no ato da entrega/instalação do(s) material(is) e/ou equipamento(s), para efeito de posterior verificação da conformidade do objeto com a especificação;

21.3.2. DEFINITIVAMENTE, após verificação de que o material entregue possui todas as características consignadas neste Edital, no que tange a quantidade solicitada e qualidade do produto especificada no Edital, no prazo de 15 (quinze) dias, contados do recebimento provisório, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes no Termo de Referência e proposta vencedora.

21.4. Após o recebimento definitivo do objeto, será atestada a Nota Fiscal para efeito de pagamento.

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

21.6. Se a Licitante vencedora deixar de entregar o material e/ou equipamento dentro do prazo estabelecido sujeitar-se-á às penalidades impostas neste Edital e no Decreto Distrital nº 26.851/2006.

22. DO PAGAMENTO

22.1. Para efeito de pagamento, a CONTRATADA deverá apresentar os documentos abaixo relacionados:

a) Prova de Regularidade junto à **Fazenda Nacional** (Débitos e Tributos Federais), à **Dívida Ativa da União** e junto à **Seguridade Social** (contribuições sociais previstas nas alíneas "a" a "d" do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991 – contribuições previdenciárias e as às de terceiros), fornecida por meio da Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União;

b) Certificado de Regularidade perante o FGTS, fornecido pela Caixa Econômica Federal, devidamente atualizado, nos termos da Lei nº 8.036, de 11/05/1990;

c) Certidão de regularidade relativa a débitos inadimplidos perante a Justiça do Trabalho (CNDT), mediante a apresentação de certidão negativa, em plena validade, que poderá ser obtida no site ***www.tst.jus.br/certidao***;

d) Prova de regularidade com a Secretaria de Estado de Economia do Distrito Federal, que poderá ser obtida por meio do site ***www.fazenda.df.gov.br***.

22.2. Para as comprovações elencadas no item **22.1**, serão aceitas certidões positivas com efeito de negativa.

22.3. Os documentos elencados no item **22.1** poderão ser substituídos, no todo ou em parte, pelo SICAF.

22.4. A Nota Fiscal deverá ser emitida em nome do **FUNDO DE SEGURANÇA PÚBLICA DO DISTRITO FEDERAL, CNPJ: 33.158.099/0001-03.**

22.5. As Notas Fiscais emitidas com dados (razão social ou CNPJ) divergentes dos informados no item **22.4**, não serão aceitas.

22.6. O pagamento será efetuado até 30 (trinta) dias, contados a partir da data de apresentação da Nota Fiscal, desde que o documento de cobrança esteja em condições de liquidação de pagamento.

22.7. A Nota Fiscal apresentada para fins de pagamento deve ser emitida pelo mesmo CNPJ constante na proposta de preços, **à exceção de empresas que sejam matriz e filial** (Acórdão nº 3.056/2008 – TCU – Plenário);

22.8. As Notas Fiscais apresentadas com CNPJ divergente da proposta de preços, **à exceção de empresas matriz e filial** (item **22.11**, *in fine*), serão devolvidas pela Administração, para a devida correção (emissão de Nota Fiscal com o CNPJ correto).

22.9. Os documentos de cobrança rejeitados por erros ou incorreções em seu preenchimento deverão ser reapresentados num prazo máximo de 5 (cinco) dias úteis, devidamente escoimados das causas que motivaram a rejeição.

22.10. 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 com a variação "*pro rata tempore*" do IPCA (art. 2º do Decreto Distrital nº 37.121/2016).

22.11. 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.

22.12. Nenhum pagamento será efetuado à Contratada enquanto pendente de apuração acerca de quaisquer descumprimentos contratuais constatados, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária (quando for o caso).

22.13. Os pagamentos, pela SSPDF, de valores iguais ou superiores a R$ 5.000,00 (cinco mil reais) serão feitos, exclusivamente, mediante crédito em conta corrente, em nome do beneficiário, junto ao Banco de Brasília S/A – BRB (Decreto Distrital nº 32.767, de 17 de fevereiro de 2011).

22.14. Excluem-se das disposições do item **22.13**:

a) pagamentos a empresas vinculadas ou supervisionadas pela Administração Pública federal;

b) os pagamentos efetuados à conta de recursos originados de acordos, convênios ou contratos que, em virtude de legislação própria, só possam ser movimentados em instituições bancárias indicadas nos respectivos documentos;

c) os pagamentos a empresas de outros Estados da federação que não mantenham filiais e/ ou representações no DF e que venceram processo licitatório no âmbito deste ente federado.

23. DAS SANÇÕES ADMINISTRATIVAS

23.1. O descumprimento de quaisquer cláusulas ou condições do presente Edital de Pregão Eletrônico e do contrato dele decorrente, em face do disposto no art. 49 do Decreto Federal nº 10.024/2019 e nos arts. 81, 86, 87 e 88 da Lei nº 8.666/93, ensejará a aplicação de penalidade que obedecerá às normas estabelecidas no **Decreto Distrital nº 26.851/2006** e alterações posteriores (**Anexo V ao Edital**).

23.2. A aplicação de qualquer das penalidades previstas no Edital (Anexo V) e no contrato realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao Licitante/adjudicatário.

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

23.4. As penalidades serão obrigatoriamente registradas no SICAF.

24. DAS DISPOSIÇÕES GERAIS

24.1. A SSPDF poderá, na hipótese de ocorrência de fatos supervenientes à publicação do Edital que possam interferir no andamento do processo ou influir na formulação da proposta, adotar uma das seguintes providências:

24.1.1. adiamento ou suspensão da licitação;

24.1.2. revogação ou anulação deste Edital, ou, ainda, sua modificação no todo ou em parte; ou

24.1.3. alteração das condições no processo licitatório, com a sua divulgação ou a republicação deste Edital, e, caso seja necessário, o estabelecimento de nova data para a realização da licitação.

24.2. A anulação da licitação induz à do contrato.

24.3. A anulação da licitação por motivo de ilegalidade não gera obrigação de indenizar.

24.4. É facultado ao Pregoeiro ou à autoridade superior, em qualquer fase da licitação, 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.

24.5. 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.

24.6. Na contagem dos prazos estabelecidos neste Edital e seus anexos, observar-se-á o que se segue:

a) Excluir-se-á o dia do início e incluir-se-á o do vencimento;

b) Os prazos somente serão iniciados e vencidos em dias de expediente na SSPDF.

24.7 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.

24.8. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse público, o princípio da isonomia, a finalidade e a segurança da contratação.

24.9. A critério do Pregoeiro, o prazo de 2 (duas) horas para o envio da proposta de preços e da documentação de habilitação poderá ser prorrogado pelo tempo que se julgar necessário.

24.10. O Licitante é o responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato, sem prejuízo das demais sanções cabíveis.

24.11. A simples apresentação de documentação não envolve qualquer compromisso de contratação por parte da Administração, importando, porém, para o Licitante a irrestrita e irretratável aceitação das condições de qualificação e dos termos deste Edital.

24.12. O Edital será disponibilizado, na íntegra, no endereço eletrônico ***https://www.gov.br/compras/pt-br/*** e também na página da SSPDF (***www.ssp.df.gov.br/licitacoes***).

24.13. O inteiro teor do processo eletrônico está disponível para vista aos interessados por meio de disponibilização de acesso externo no SEI (serviço eletrônico de informações).

24.14. O pedido de vista deverá ser encaminhado à Subsecretaria de Administração Geral através do e-mail licitacoes@ssp.df.gov.br.

24.15. Os casos omissos e demais dúvidas suscitadas serão dirimidos pelo Pregoeiro, no endereço eletrônico mencionado neste Edital, **item 4**, através do fone (61) 3441-8824 ou diretamente na Coordenador de Planejamento, Licitações e Compras Diretas – SAM, Quadra "A", Bloco "A", CEP 70620-000, Brasília/DF.

24.16. O foro de Brasília – DF, com exclusão de qualquer outro, por mais privilegiado que seja, será o designado para julgamento de quaisquer questões judiciais resultantes da presente licitação e da aplicação do presente Edital.

24.17. As Licitantes deverão comprovar, caso cabível, o atendimento da Lei Distrital nº 4.652/2011, que cria, no âmbito do DF, o Programa de Valorização Profissional junto aos apenados em regime semiaberto e aos egressos do Sistema Penitenciário.

25. ANEXOS

25.1. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

25.1.1. ANEXO I – Termo de Referência;

25.1.2. ANEXO II – Declaração de Sustentabilidade Ambiental (art. 7º da Lei Distrital nº 4.770/2012);

25.1.3. ANEXO III - Declaração para os fins do Decreto nº 39.860, de 30 de maio de 2019

25.1.4. ANEXO IV – Minuta de Contrato de Aquisição de Bens (entrega integral);

25.1.5. ANEXO V – Decreto Distrital nº 26.851/2006 – regulamentação de penalidades no âmbito do DF.

25.1.6. ANEXO VI - Modelo de Declaração de que é beneficiário do Decreto nº 7.174/2010.

Havendo irregularidades neste instrumento, entre em contato com a Ouvidora de Combate à Corrupção, no telefone 0800-6449060, nos termos do Decreto nº 34.031, de 12 de dezembro de 2012 (DODF 252, de 13/12/2012).

AMILCAR UBIRATAN URACH VIEIRA

Coordenador de Planejamento, Licitações e Compras Diretas

CELSO WAGNER LIMA

Subsecretário de Administração Geral

ANEXO I AO EDITAL

TERMO DE REFERÊNCIA

TERMO DE REFERÊNCIA

PROCESSO SEI-GDF Nº: 00050-00010540/2022-39

ELEMENTO DE DESPESA: 44.90.52.63 e 33.90.40.11

REGIME DE EXECUÇÃO: Fornecimento Integral (de uma só vez).

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de empresa especializada para fornecer solução de segurança compota por Firewall, do tipo NGFW, de alta capacidade para Segurança de datacenter, firewalls de pequeno porte, gerência centralizada de logs e eventos dos firewall e antivírus com EDR com instalação, configuração, suporte técnico, manutenção e garantia de 36 (trinta e seis) meses, conforme especificações, quantitativos e condições estabelecidas neste Termo de Referência (TR) e seus anexos.

2. DETALHAMENTO DO OBJETO

GRUPO	BEM/SERVIÇOS	ITEM	CATMAT/CATSER	DESCRIÇÃO	QUANTIDADE
1	Solução de Firewall	1	27502	Tipo I - Firewall NGFW *Licença UTP para equipamento FG-1500D, ou NGFW de outro fabricante que atue na proteção da comunicação das LANs da SSPDF, WAN e Internet	2
		2	150100	Tipo II - Firewall NGFW	3
		3	150100	Gerência Centralizada de Logs e Eventos	1
2	Solução de Antivírus	4	27499	Licença Antivirus Desktop	500
		5	27499	Licença Antivirus Servidor	300

2.1. Os objetos desta contratação são caracterizados como comuns, uma vez que possuem padrões de desempenho e qualidade objetivamente definidos, mediante especificações usuais adotadas no mercado, de forma a permitir aos potenciais fornecedores do ramo de atividade compatível com o objeto da licitação condições de ofertarem suas propostas, sendo possível a comparação objetiva das mesmas tendo como critério de julgamento o menor preço sem comprometimento da qualidade desejada.

3. FUNDAMENTAÇÃO LEGAL DA CONTRATAÇÃO

3.1. O presente termo de referência foi planejado e elaborado com fundamentos nos seguintes dispositivos legais.

3.2. **Lei nº 8.078/1990**, que estabelece normas de proteção e defesa do consumidor;

3.3. **Lei nº 8.666/1993**, que regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

3.4. **Lei nº 10.520/2002**, que 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;

3.5. **Lei Complementar nº 123/2006**, que institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte; altera dispositivos das Leis nº 8.212 e nº 8.213, ambas de 24 de julho de 1991, da Consolidação das Leis do Trabalho - CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, da Lei nº 10.189, de 14 de fevereiro de 2001, da Lei Complementar nº 63, de 11 de janeiro de 1990; e revoga as Leis nº 9.317, de 5 de dezembro de 1996, e nº 9.841, de 5 de outubro de 1999;

3.6. **Decreto Federal nº 10.024/2019**, que regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal, recepcionado no âmbito da administração direta e indireta do Distrito Federal, por meio do Decreto distrital nº 40.205/2019;

3.7. **Decreto Federal nº 7.174/2010**, que 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;

3.8. **Decreto Federal nº 9.412/2018**, que atualiza os valores das modalidades de licitação de trata o art. 23 da Lei nº 8.666, de 21 de junho de 1993.

3.9. **Lei Distrital nº 4.611/2011**, que regulamenta no Distrito Federal o tratamento favorecido, diferenciado e simplificado para microempresas, empresas de pequeno porte e microempreendedores individuais de que trata a Lei Complementar nº 123, de 14 de dezembro de 2006, as Leis Complementares nº 127, de 14 de agosto de 2007, e nº 128, de 19 de dezembro de 2008, e dá outras providências;

3.10. **Lei Distrital nº 4.770/2012**, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens e na contratação de obras e serviços pelo Distrito Federal;

3.11. **Lei Distrital nº 5.525/2015**, que estabelece que, em compras e contratações de bens e serviços, qualquer que seja a modalidade de licitação, o valor a ser pago não seja superior à média de preços do mercado, no âmbito do Distrito Federal, e dá outras providências;

3.12. **Decreto Distrital nº 23.287/2002**, que aprova modelo de Termos-Padrão e serem utilizados no âmbito do Distrito Federal e dá outras providências;

3.13. **Decreto Distrital nº 23.460/2002**, que regulamenta a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, instituída pela Lei Federal nº 10.520/2002;

3.14. **Decreto Distrital nº 26.851/2006,** que regulamenta a aplicação de sanções administrativas previstas na Lei nº. 8.666/1993;

3.15. **Decreto Distrital nº 32.598/2010**, que aprova as Normas de Planejamento, Orçamento, Finanças, Patrimônio e Contabilidade do Distrito Federal, e dá outras providências;

3.16. **Decreto Distrital nº 32.767/2011**, que dispõe sobre a regulamentação para a movimentação dos recursos financeiros alocados à "Conta Única" do Tesouro do Distrito Federal, e dá outras providências.

3.17. **Decreto Distrital nº 33.608/2012**, que exclui do regime de centralização das licitações de compras, obras e serviços de que trata o art. 2º da Lei nº 2.340, de 12 de abril de 1999, os procedimentos licitatórios de interesse da Secretaria de Estado de Segurança Pública do Distrito Federal, e dá outras providências;

3.18. **Decreto Distrital nº 35.592/2014,** que regulamenta o tratamento preferencial e simplificado nas contratações públicas das microempresas, empresas de pequeno porte e microempreendedores individuais previsto na Lei nº 4.611/2011, estabelece regras para a elaboração do Plano Anual de Contratações Públicas para ampliação da participação das denominadas entidades preferenciais, e dá outras providências;

3.19. **Decreto Distrital nº 36.520/2015,** que estabelece diretrizes e normas gerais de licitações, contratos e outros ajustes para a Administração Direta e Indireta do Distrito Federal e dá outras providências;

3.20. **Decreto Distrital nº 37.121/2016**, que dispõe sobre a racionalização e o controle de despesas públicas no âmbito do Distrito Federal;

3.21. **Decreto Distrital nº 37.667/2016,** que dispõe sobre a contratação de bens e serviços de Tecnologia da Informação no âmbito da Administração Direta e Indireta do Distrito Federal, e dá outras providências;

3.22. **Decreto Distrital nº 39.103/2018**, que regulamenta, no âmbito do Distrito Federal, o sistema de Registro de preço e dá outras providencias;

3.23. **Decreto Distrital nº 39.453/2018**, que regulamenta a Lei distrital nº 5.525, de 26 de agosto de 2015, que estabelece que, em compras e contratações de bens e serviços, qualquer que seja a modalidade de licitação, o valor a ser pago não seja superior à média de preços do mercado, no âmbito do Distrito Federal;

3.24. **Decreto Distrital nº 39.860/2019,** que dispõe sobre a proibição de participação, direta ou indiretamente, de licitação, contratação, execução de obra ou serviço e do fornecimento de bens a eles necessários agentes públicos de órgãos ou entidades da Administração Pública Direta ou Indireta do Poder Executivo do Distrito Federal contratante ou responsável pela licitação;

3.25. **Decreto Distrital nº 40.205/2019**, que recepciona o Decreto Federal nº 10.024, de 20 de setembro de 2019.

3.26. **Portaria nº 514/2018/SEFP**, que regulamenta os procedimentos administrativos básicos para realização de pesquisa de preços na aquisição de bens e contratação de serviços em geral na forma do Decreto Distrital nº 39.453, de 14 de novembro de 2018;

3.27. **Portaria nº 356/2019**, que estabelece os procedimentos de verificação previstos no art. 5º do Decreto nº 39.860, de 30 de maio de 2019;

3.28. **Portaria nº 247/2019 - SEEC/DF**, que aprova o manual do Imposto de Renda Retido na Fonte, de titularidade do Distrito Federal, nos termos do art. 157, inciso I, da Constituição da República Federativa do Brasil de 1988;

3.29. **Portaria nº 119, de 04 de setembro de 2019** Estabelece diretrizes para a gestão, acompanhamento e fiscalização da execução de contratos, convênios, acordos e instrumentos congêneres celebrados pela Secretaria de Estado de Segurança Pública do Distrito Federal, e dá outras providências;

3.30. **Instrução Normativa SGD/ME nº 01, de 4 de abril de 2019** e seus Anexos: dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

3.31. **Decreto Distrital nº 44.613/2023**, que fixa o regime de transição de que trata o art. 191 da Lei nº 14.133, de 1º de abril de 2021, alterado pela Medida Provisória nº 1.167, de 31 de março de 2023, no âmbito da Administração Pública direta, autárquica e fundacional do Distrito Federal.

4. JUSTIFICATIVAS DA CONTRATAÇÃO

4.1. **Contexto Interno**

4.1.1. A Secretaria de Estado de Segurança Pública do Distrito Federal (SSP/DF) teve sua origem no Decreto Distrital Nº 4.852, de 11 de Outubro de 1979 e tem como principal compromisso centralizar e comandar as ações dos órgãos de segurança pública para atividades policiais primordialmente preventivas e de participação comunitária, visando a proteção do cidadão, garantindo assim a melhoria da qualidade de vida da população.

4.1.2. Compete à SSP/DF propor e implementar toda a política de segurança pública determinada pelo Governo do Distrito Federal, objetivando a racionalização dos meios operacionais na busca pela maior eficácia do sistema de segurança pública do DF. Para isso, cabe a essa Secretaria a missão de planejar, coordenar e supervisionar o emprego operacional das forças de segurança como a Polícia Militar, a Polícia Civil, o Corpo de Bombeiros Militar e do Departamento de Trânsito, sem interferir na autonomia funcional, administrativa e financeira dessas instituições.

4.1.3. A SSPDF Pública possui em operação dezenove sistemas informatizados de gestão que utilizam a Internet, com o objetivo de dar suporte às áreas operacionais e administrativas, dentre eles o SGO versão 2.0, responsável pelo controle e integração entre Agências de segurança pública e atendimento de chamados de emergência (CBMDF, PMDF, PCDF, Defesa Civil), atividades estas finalísticas da SSP/DF por corresponderem a ações essenciais e vitais ao cumprimentos de suas atribuições. Além do exponencial crescimento do PVU(Projeto de Videomonitoramento Urbano) que está em expansão para novas áreas do DF.

4.1.4. O Sinesp CAD é uma solução de suporte ao serviços emergenciais, que permite a integração do atendimento das Forças de Segurança Pública e outros órgãos (Polícia Militar do Distrito Federal, Polícia Civil do Distrito Federal, Corpo de Bombeiros Militar do Distrito Federal, SAMU, DER, CAESB, etc) otimizando recursos e diminuindo o tempo resposta ao cidadão, além de melhorar o planejamento operacional. Ele fornece aos profissionais de segurança pública uma solução de Tecnologia da Informação que permite o atendimento à ocorrências solicitadas a partir de números tridígitos emergenciais (190, 191, 192, etc) ou de outros canais de acionamento de atendimento ao cidadão, abarcando os processos de atendimento, despacho e fechamento dos atendimentos, além da integração entre as agências de segurança pública.

4.1.5. Outro serviço prestado é o aplicativo Viva Flor, que é um sistema de segurança preventiva para mulheres vítimas de violência doméstica ou familiar que estejam sob o resguardo de medida protetiva de urgência. O dispositivo é instalado no celular da ofendida e permite, nos casos classificados como de risco extremo, a possibilidade de acionar a polícia com apenas um toque na tela inicial do aparelho. As vítimas dispõem, a partir daí, de atendimento prioritário em situação de emergência. O principal objetivo do programa é oferecer mais uma ferramenta de proteção, com absoluta prioridade no atendimento.

4.1.6. Dentro da estrutura do SOPI, foi inaugurado em julho de 2018 por força do Decreto 38.998 de 19/04/2018, o Centro Integrado de Operações de Brasília - CIOB, um organismo multiagência concebido sob os moldes de um C4I (Comando, Controle , Comunicações, Computação e Inteligência) que reúne 22 órgãos, instituições e agências do DF, com foco na segurança pública, mobilidade, fiscalização, serviços e saúde e que tem por objetivo principal promover a coordenação e integração dos diversos órgãos que atuam de forma interdependente na administração direta e indireta no Distrito Federal e ainda, alcançar maior eficiência em suas ações e integrar várias secretarias e agências e outros setores da Administração Pública do Distrito Federal.

4.1.7. Além de ser o principal articulador com os órgãos que compõem o Sistema de Segurança Pública do DF, a SSP/DF trabalha também junto aos demais setores do Governo do Distrito Federal e junto à sociedade civil para colocar em prática ações de enfrentamento ao crime organizado e à violência, por meio de ações preventivas e de participação comunitária, bem como a de repressão qualificada, visando a manutenção da segurança e da ordem no contexto do Distrito Federal.

4.1.8. Sob a diretriz e comando da SSP-DF, as operações atualmente realizadas neste centro integrado, tem como características a polivalência, a agilidade e a rapidez no compartilhamento das informações a todas as forças diretamente envolvidas em cada ocorrência, ou seja; este Centro é hoje a principal porta de entrada das chamadas de atendimentos e ocorrências oriundas dos canais de atendimento e das forças de Segurança, transformando-se assim na mais segura e confiável interface entre a sociedade e a Secretaria de Segurança Pública do Distrito Federal.

4.1.9. Em sua estrutura organizacional, a SSP/DF é composta por diversas Subsecretarias, sendo uma destas a Subsecretaria de Operações Integradas - SOPI, que tem como atividades principais: planejar, coordenar, executar e avaliar as atividades de Segurança Pública, implementando normas e diretrizes específicas para orientar o emprego operacional em determinadas ações. Além dessas atribuições é também responsabilidade da SOPI:

4.1.10. Cadastrar, fiscalizar e controlar órgãos, entidades, estabelecimentos comerciais e pessoas jurídicas de direito privado que tenham atividades sujeitas ao controle ou fiscalização da SSP/DF;

4.1.10.1. Cadastrar empresas de Segurança Privada, de coletes balísticos a blindagem de carros e

4.1.10.2. Cadastrar eventos, como shows artísticos, jogos, corridas e manifestações populares que demandem a ação dos órgãos de segurança pública.

4.1.11. Outro fato que justifica o acima exposto e sua essa necessidade é o fato de que caberá a SSP-DF, na qualidade de órgão centralizador e integrador das ações e iniciativas de Segurança, ser o controlador e protagonista no **Projeto de Vídeo Monitoramento Urbano (PVU)** de todas as regiões do DF.

4.1.12. As operações de monitoramento ocorrem sob o regime 24 (vinte e quatro) horas por dia nos 7 (sete) dias da semana. Os recursos tecnológicos necessários para atenderem essa demanda deverão ser providos da mais alta tecnologia disponível e devem funcionar de forma ininterrupta, pois, em caso de qualquer parada, esses serviços de urgência ou emergência poderão ficar indisponíveis, penalizando assim o cidadão que reside no Distrito Federal e que confia e se vale desses serviços.

4.1.13. As atividades de vídeo monitoramento previstas no **PVU** possuem a finalidade, somada a outras iniciativas, de garantir uma resposta acurada, rápida e eficaz decorrentes da apuração e validação das imagens dos eventos em tempo real, combatendo assim com inteligência qualificada a criminalidade, propiciando a redução dos índices de crimes violentos, a diminuição dos crimes letais intencionais e dos crimes contra o patrimônio, o que gera, em consequência, o aumento da credibilidade das instituições de segurança pública e da sensação de segurança da comunidade do Distrito Federal.

4.1.14. Ocorre que atualmente o número de câmeras instaladas e disponíveis não cobrem todas as áreas do DF, estando o projeto em acelerada fase de expansão; saindo dos atuais 959 (novecentos e cinquenta e nove) equipamentos/câmeras em funcionamento para aproximadamente 1.500 (mil) equipamentos/câmeras com previsão para que este número seja alcançado no final de 2023. Para contornar este obstáculo, faz-se necessária e imperativa a ampliação e modernização tecnológica da atual arquitetura de trafego e gestão da informação e de sua infra estrutura (incluindo o armazenamento seguro das imagens geradas), com tecnologia adequada para atender toda a demanda.

4.1.15. Dessa forma, verificamos que a não atualização do parque tecnológico, bem como a falta de contrato de garantia e substituição de peças dos equipamentos que compõem este sistema é um entrave que certamente causará pesados prejuízos ao modelo da solução adotada e na consequente continuidade dos serviços por falha nestes equipamentos, devido ao desgaste natural; acarretando na impossibilidade do pronto restabelecimento dos serviços. Para mitigar tal ocorrência, as boas práticas de governança de Tecnologia da Informação e Comunicação (TIC) recomendam que o parque tecnológico, em situação de missão crítica, que exija a alta disponibilidade dos recursos; permaneça sempre atualizado, com configurações adequadas e coberto por contratos de garantia, substituição de peças e a correta manutenção de equipamentos.

4.1.16. Por esse motivo, faz-se necessária a imediata atualização dos equipamentos de infraestrutura de rede utilizados para suportar os serviços hoje prestados pelos sistemas de segurança pública do DF e órgãos sob a gestão da SSP-DF, pois essa atualização contribuirá positivamente tanto na efetivação dos serviços como nas demais atividades administrativas, diretas e indiretas, além de fornecer recursos de suporte para a realização de fiscalização das atividades de campo (monitoramento de eventos, shows, manifestações, jogos, entre outros).

4.1.17. Feito este registro, evidencia-se ainda mais a necessidade e a essencialidade de uma solução de Segurança (firewall), que preze pela integridade, inviolabilidade e robustez face a alta disponibilidade e exigências dos serviços que se utilizam da infraestrutura de Tecnologia da Informação, para garantir a segurança da rede corporativa, assim como todos os sistemas vinculados à SSP/DF, ao público interno e externo. Esta contratação é fundamental para a continuidade dos serviços prestados as forças de segurança do Distrito Federal e por extensão ao cidadão, preservando as informações críticas ao negócio, bem como garantindo a proteção da infraestrutura tecnológica com vistas a possibilitar ambiente seguro e estável da rede de dados.

4.2. **Contexto Externo**

4.2.1. Cenários de Invasões externas a sites do governo indicam que soluções de segurança deve estar atualizadas e preparadas para novas formas de ataques hacker.

4.2.2. Os cuidados com o tratamento de dados pessoais e sua proteção prevista LGPD exigem que a corporação possua ferramentas capaz de realizar essas proteções e mitigar possíveis falhas e vazamento de dados.

4.3. **DA JUSTIFICATIVA**

4.3.1. A SSP/DF convive com problemas estruturais e de concepção desde a sua criação em 1979, ainda que estes problemas tenham sido em pequena parte contornados por conta das incumbências e demandas referentes aos planejamentos e ações de segurança relacionadas aos grandes eventos (Copa do Mundo e Olimpíadas), os equipamentos hoje utilizados encontram-se defasados e tal defasagem tem como causa os seguintes fatores a saber: desgaste natural (pelo uso continuo/efetivo e tempo de utilização), fim da vida comercial ou *End of Life* de muitos equipamentos e o fim da disponibilidade de peças de reposição. Evidencia-se assim a necessidade de substituição de muitos desses equipamentos em virtude de completa impossibilidade de reparo ou de sua manutenção adequada visando a continuidade dos serviços prestados.

4.3.2. A segurança da informação tem como base três pilares: **confidencialidade, integridade e disponibilidade,** para garantir a tríade da segurança da informação faz-se necessário possuir equipamentos de segurança sempre atualizados e com suporte e garantia do fabricante. Nesse sentido alguns dos equipamentos que a SSPDF possui, já não conta mais com o suporte do fabricante, não sendo possível a atualização e extensão de garantias e outros ainda é possível a atualização e expansão de garantias pelo fabricante.

4.3.3. Considerando a necessidade de atualização da infra estrutura de rede desta Secretaria, etapa esta que já se encontra em curso e alinhado aos requisitos de negócio das unidades vinculadas a SSP/DF, para a implantação de alta disponibilidade. Juntando-se a esse escopo, está prevista a inclusão do Projeto de Vídeo Monitoramento Urbano - PVU, que resultará em maior trafego de rede e consequentemente numa maior necessidade de segurança e gestão.

4.3.4. Existe hoje a necessidade desta Secretaria, em continuar provendo alta disponibilidade, integridade e confidencialidade em seus sistemas de informação, com recursos computacionais e equipamentos capazes de enfrentar os desafios diários que surgem de uma Internet cada vez mais insegura, onde novas técnicas de invasão emergem a cada dia. A captura de informações por parte de pessoas e grupos mal intencionados viraram rotina. Assim os órgãos se Segurança Pública necessitam manter se atualizados e preparados tecnologicamente para enfrentar essas tentativas de invasão em suas redes e a possível captura de dados sensíveis

4.3.5. A rede da SSP/DF apresenta crescente demanda no monitoramento por vídeo, além da necessidade de promover segurança da informação personalizada para: grupos de usuários, servidores, estações de trabalho, portas, protocolos e aplicações.

4.3.6. Ressaltando-se que como o objetivo de toda estrutura redundante em TI, o objetivo principal é garantir de forma ininterrupta a continuidade na prestação dos serviços e evitar assim a perda de dados. Isso é feito com tecnologias inteligíveis, múltiplos locais de armazenamento de dados e fontes de energia em duplicidade. Todo esse esforço é feito no sentido de se evitarem falhas e indisponibilidades na rede de dados e consequentemente nos sistemas desta Secretaria, que caso ocorram, irão causar severos danos, principalmente quando afetam os serviços relacionados com a segurança dos dados trafegados e os de emergência essenciais à população.

4.3.7. Do ano de 2020 veio a lição de que com o advento da Pandemia provocada pelo SARS Covid 19, surge a necessidade de se manter um ambiente dual para os usuários trabalharem com segurança e eficiência em locais fora da Sede física da SSP/DF, através de conexões de Rede Privada Virtual (VPN - do inglês Virtual Private Network). A utopia de um trabalho home office virou uma realidade que hoje precisa ser considerada e prevista para todo e qualquer projeto de arquitetura consciente e responsável de uma rede.

4.3.8. Conclui-se assim que é primordial a aquisição de solução de segurança computacional composta por firewall e antivirus, garantindo a funcionalidade e continuidade dos serviços de forma incessante.

4.4. **Resultados e benefícios a serem alcançados**

4.4.1. Prover a Secretaria de Segurança Pública com segurança cibernética contra ataques digitais oriundos de redes de comunicação externas e internas;

4.4.2. Reduzir a probabilidade de indisponibilidade dos serviços prestados por esta Secretaria devido à ataques cibernéticos;

4.4.3. Controle e visibilidade de acessos realizados aos serviços prestados por esta Secretaria;

4.4.4. Manutenção e progressão da confiabilidade dos dados prestados por esta Secretaria;

4.4.5. Manutenção da integridade, confidencialidade e disponibilidade de informações de caráter sigiloso;

4.4.6. Atualização do parque tecnológico quanto a itens de segurança cibernética;

4.4.7. Manutenção de conformidade quanto às melhores práticas de mercado quanto à segurança cibernética.

4.5. **Alinhamento Estratégico**

4.5.1. O objeto da contratação está previsto no Plano de Contratações Anual 2023 - SMT:

Cód.	Objeto
SMT-61	Aquisição de firewall 36 meses
SMT-69	Aquisição de antivírus 36 meses

4.5.2. O objeto da contratação também está alinhado com a Estratégia da SSP/DF e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) da SSP/DF:

Plano de Ações de Segurança da Informação e Comunicações do PPA da SSP – DF

Cód.	Objetivos
SI03	Modernizar e manter solução de Firewall
SI04	Modernizar e manter End Point Protection (Antivírus)

Metas do PPA para SSP-DF (2020-2023)

Metas do PPA	Referência
Necessidade de providenciar infraestrutura adequada para que as áreas de negócio consigam executar suas atribuições com o devido suporte de TI	N01

5. JUSTIFICATIVA DA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

5.1. O Estudo Técnico Preliminar (125895467) foi elaborado conforme as diretrizes constantes no Decreto nº 10.024/2019 e demais normativos que disciplinam os serviços a serem contratados ou bens a serem adquiridos, buscado melhorar a conclusão que viabilize a pretensa contratação e servindo, assim, para fundamentar o presente Termo de Referência.

6. JUSTIFICATIVA DO OBJETO DA CONTRATAÇÃO SER SERVIÇO COMUM E DA MODALIDADE DE LICITAÇÃO

6.1. É possível observar, diante das especificações contidas neste Termo de Referência que o objeto almejado possui padrões de desempenho e qualidade objetivamente definidos, mediante especificações usuais adotadas no mercado, de forma a permitir aos potenciais fornecedores do ramo de atividade compatível com o objeto da licitação condições de ofertarem suas propostas, sendo possível a comparação objetiva das mesmas tendo como critério de julgamento o menor preço sem comprometimento da qualidade desejada, a exemplo das propostas que foram levantadas para balizamento de preços; logo vislumbra-se para o presente certame que o objeto da licitação pode ser considerado comum, sendo portanto, aplicável a modalidade pregão em sua forma eletrônica.

7. JUSTIFICATIVA DO AGRUPAMENTO DO OBJETO DA CONTRATAÇÃO

7.1. O presente Termo foi elaborado com o agrupamento do objeto em grupos. O TCU se manifestou sobre o tema através da Súmula 247 - TCU/2007 (grifo nosso):

> "*É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível,* ***desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala****, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade ".*

7.2. No presente caso, o agrupamento de itens encontra respaldo por haver total correlação/compatibilidade, de forma que encontra-se em consonância inclusive com as regras de mercado para a comercialização dos produtos, de modo a manter a competitividade necessária à disputa.

8. JUSTIFICATIVA NA ADOÇÃO DO SIGILO DO ORÇAMENTO-BASE

8.1. O decreto Nº 10.024/19, estabelece que o valor máximo aceitável ou valor estimado das aquisições ou contratações poderão ser sigilosos. Em razão disso, adotamos a forma sigilosa para a presente contratação, pois, nessa etapa da contratação os licitantes ofertaram preços condizentes com o valor de mercado dos produtos pretendidos pela Administração Pública, observando assim princípios públicos como: eficiência, eficácia, economicidade. Essa opção do sigilo no orçamento-base no valor dos produtos pretendidos pelo ente público não possibilita o conhecimento prévio pelos licitantes do valor estimados na pesquisa mercadológica realizada pela administração pública, espera-se que a adoção dessa pratica legal restrinjam preços superfaturados e, consequentemente, prejuízo para Estado, e, que as as empresas apresentem propostas mais realistas economicamente.

8.2. Assim, em razão do objeto desse Termo de Referência ser de baixa complexidade para contratação e com inúmeras empresas que trabalham com esses equipamentos, optamos pela adoção do sigilo do orçamento-base para que os preços ofertados pelas empresas participantes do certame aproximem-se dos valores praticados do mercado evitando compras públicas com preços superfaturados.

9. JUSTIFICATIVA DA NÃO UTILIZAÇÃO DO SISTEMA DE REGISTRO DE PREÇOS

9.1. A presente aquisição não será processada pelo Sistema de Registro de Preços, em razão do objeto não se enquadrar no disposto nos incisos I, II, III e IV, art. 3º, do Decreto distrital nº 39.103/2018, por se tratar de aquisição única, com a entrega do bem previamente definida em quantidades certas neste Termo de Referência e com previsão de recursos orçamentário para fazer face à despesa.

9.2. O presente processo de aquisição não se enquadra nos pré-requisitos acima citados por se tratar de aquisição com entrega integral (todo quantitativo de uma só vez) em quantidade previamente definida neste Termo de Referência, afastando a aplicação do Sistema de Registro de Preços na forma do art. 3º, incisos I, II e IV, do Decreto distrital nº 39.103/2018, uma vez que não haverá necessidade de contratações frequentes ou entregas parceladas não definidas e, ainda, por ser possível definir previamente o quantitativo a ser demandado por esta Administração.

9.3. Por outro lado, a presente aquisição não se enquadra, igualmente no inc. III do art. 3º, do Decreto distrital nº 39.103/2018. Não há que se falar em atendimento de demandas de outros órgãos da Administração do Distrito Federal, tendo em vista que a SSP/DF, foi excluída do regime de centralização das licitações de compras, obras e serviços, por meio Decreto distrital nº 33.608/2012, para adotar procedimentos licitatórios de interesse da Pasta.

10. JUSTIFICATIVA DA RESTRIÇÃO DE PARTICIPAÇÃO DE EMPRESAS CONSORCIADAS, PESSOAS FÍSICAS NÃO EMPRESÁRIAS E DE SUBCONTRATAÇÃO

10.1. Não será permitida a participação de empresas consorciadas e a subcontratação, uma vez que não há complexidade para a aquisição do bem objeto do certame em tela, não havendo justificativa para a permissão de empresas participarem em consórcio ou a subcontratação, o que fundamenta tal impedimento visto que a amplitude do objeto almejado ou a diversidade de elementos que o compõem não evidenciam dificuldade de o objeto ser implementado.

10.2. Não é possível a participação de pessoas físicas não empresárias neste certame, uma vez que não possuem os requisitos mínimos indispensáveis para o fornecimento do objeto deste Termo de Referência (TR), não havendo como verificar a documentação de habilitação jurídica, fiscal e qualificação técnica, entre outras, por não possuírem tais documentos.

11. JUSTIFICATIVA DO NÃO TRATAMENTO PREFERENCIAL E SIMPLIFICADO NAS CONTRATAÇÕES PÚBLICAS DAS MICROEMPRESAS, EMPRESAS DE PEQUENO PORTE E MICROEMPREENDEDORES INDIVIDUAIS

11.1. A Lei Complementar nº 123/06, alterada pela Lei Complementar nº 147/2014, elencou no art. 49, algumas hipóteses que, se presentes no caso concreto, dispensam ou eximem a autoridade responsável pela licitação de aplicar os benefícios materiais previstos nos arts. 47 e 48 do mesmo diploma legal. Assim, vale a máxima: 'para toda regra existe uma exceção'. Assim sendo, de conformidade com o art. 49, não se aplica os benefícios dos arts.47 e 48 quando:

> ... "b) o tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte não for vantajoso para a administração pública ou representar prejuízo ao conjunto ou complexo do objeto a ser contratado; ou,"...

11.2. O objetivo principal em não adotar o tratamento preferencial é o de possibilitar uma padronização no fornecimento do serviço. Considerando que o objeto almejado NÃO é de natureza divisível e que o estabelecimento de subcontratação compulsória para entidades preferenciais CAUSARÁ prejuízo para o conjunto do objeto deste certame; não será atendido o contido no art. 48, inciso III, da Lei Complementar nº 123/2006 c/c o art. 23, § 1º, e 27 da Lei Distrital nº 4.611/2011 e art. 9º do Decreto Distrital nº 35.592/2014, deixando de ser estabelecida subcontratação compulsória para entidades preferenciais (microempresas, empresas de pequeno porte e microempreendedores individuais), conforme estabelecido no art. 9º, § 11, incs. II e III, do Decreto Distrital nº 35.592/2014.

11.3. Tendo em conta o fato de que o valor referencial suplanta o limite legal de R$ 80.000,00, caberia, em tese, disputa dividida em cota principal e cota reservada a MEs/EPPs, nos termos do art. 48, III, da Lei Complementar n.º 123/2006. Todavia, o simples exame do Termo de Referência (TR) é suficiente para concluirmos que, em função da necessidade e compatibilidade entre os itens objetos da licitação em tela, torna-se inviável a reserva de cota para as ME/EPP, sob pena de tal ação resultar em prejuízo ao conjunto do objeto a ser contratado. Sendo assim, a disputa será aberta à ampla participação, com respaldo no que dispõe o art. 49, III, do Estatuto da ME/EPP. Em face disso, aplica-se somente a preferência a micros e pequenas empresas no caso de ocorrência de empate ficto, nos termos do que dispõem os arts. 44 e 45 do aludido diploma."

12. JUSTIFICATIVA DA ADOÇÃO DE PRÁTICAS DE SUSTENTABILIDADE AMBIENTAL NA EXECUÇÃO DOS SERVIÇOS

12.1. Em atenção à Lei nº 4.770/2012 serão exigidos neste certame a aplicação de critérios de sustentabilidade ambiental.

12.2. As empresas licitantes interessadas neste certame deverão se atentar quanto às obrigações estabelecidas no subitem deste Termo de Referência, que trata **DA OBRIGATORIEDADE DO USO DE CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL**.

13. PLANILHA ESTIMATIVA DE CUSTOS E VALORES DE REFERÊNCIA ESTIMADOS

13.1. **PLANILHA**

GRUPO	BEM/SERVIÇOS	ITEM	CATMAT/CATSER	DESCRIÇÃO	QUANTIDADE	INTERVALO MONETÁRIO	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Firewall	1	27502	Tipo I - Firewall NGFW *Licença UTP para equipamento FG-1500D, ou NGFW de outro fabricante que atue na proteção da comunicação das LANs da SSPDF, WAN e Internet	2	R$ 20,00	SIGILOSO	SIGILOSO
		2	150100	Tipo II - Firewall NGFW	3	R$ 20,00	SIGILOSO	SIGILOSO
		3	150100	Gerência Centralizada de Logs e Eventos	1	R$ 20,00	SIGILOSO	SIGILOSO
2	Solução de Antivírus	4	27499	Licença Antivirus Desktop	500	R$ 20,00	SIGILOSO	SIGILOSO
		5	27499	Licença Antivirus Servidor	300	R$ 20,00	SIGILOSO	SIGILOSO
TOTAL GERAL								SIGILOSO

13.2. **CUSTO ESTIMADO**

13.3. O custo estimado da contratação é de **R$ SIGILOSO**.

13.4. **NATUREZA / ELEMENTO DE DESPESA**

Grupo	Itens	Natureza/Elemento de Despesa	Valor
1	1	44.90.52-63	SIGILOSO
	2		
	3		
2	4	44.90.40-25	SIGILOSO
	5		
TOTAL			**SIGILOSO**

13.5. O valor de referência estimado do presente termo ***será sigiloso***, estando disponibilizado exclusiva e permanentemente aos órgãos de controle externo e interno e serão divulgados logo após o encerramento do envio de lances, sem prejuízo da divulgação do detalhamento dos quantitativos e das demais informações necessárias à elaboração das propostas;

13.6. Os quantitativos e respectivos códigos dos itens são os discriminados nas tabelas acima;

13.7. Em caso de discordância existente entre as especificações do objeto descrito neste Termo, com as do COMPRAS GOVERNAMENTAIS – CATMAT/CATSER, prevalecerão as especificações constantes neste Termo de Referência (TR). Para elaboração da proposta o participante deve se basear no descritivo contido no Termo de Referência (TR);

13.8. A licitante não poderá cotar quantidade inferior ao quantitativo contido neste Termo, de acordo com o acima estabelecido.

14. INTERVALO MONETÁRIO

14.1. O intervalo mínimo de diferença de valores ou de percentuais entre os lances está consignada na respectiva coluna da Tabela contida no Item anterior (Planilha de Estimativa do Valor da Contratação), atendendo ao Art. 14, inciso III do Decreto Federal nº 10.024/2019.

15. ESPECIFICAÇÕES MÍNIMAS ACEITÁVEIS E FORMA DE EXECUÇÃO DO SERVIÇO

GRUPO 1 (ITENS 1, 2 e 3)

15.1. **FIREWALL TIPO 1**

15.1.1. Os equipamentos devem ser mantidos atualizados na última versão de sistema operacional disponível pelo fabricante durante o período de vigência contratual;

15.1.2. Os equipamentos devem ser do mesmo fabricante da solução de gerenciamento centralizado de logs;

15.1.3. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/ transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/ transceptores necessários para a plena utilização;

15.1.4. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP.

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

15.1.6. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;

15.1.7. Possuir fonte de alimentação redundante e hot-swappable;

15.1.8. Possuir, no mínimo, 8 (oito) interfaces de rede 10 Gbps SFP+;

15.1.9. Possuir, no mínimo, 16 (dezesseis) interfaces de rede 1Gbps UTP;

15.1.10. Armazenamento de, no mínimo, 02 (dois) Solid State Drive (SSD) de 240 GB;

15.1.11. Throughput de, no mínimo, 9.8 Gbps, para conexões VPN;

15.1.12. Suporte a, no mínimo, 232.000 (duzentos e trinta e dois mil) novas conexões ou sessões por segundo;

15.1.13. Suporte a, no mínimo, 12.000.000 (doze milhões) de conexões ou sessões simultâneas;

15.1.14. Throughput de, no mínimo, 15 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

15.2. **FIREWALL TIPO 2**

15.2.1. Os equipamentos devem ser mantidos atualizados na última versão de sistema operacional disponível pelo fabricante durante o período de vigência contratual;

15.2.2. Os equipamentos devem ser do mesmo fabricante da solução de gerenciamento centralizado de logs;

15.2.3. Throughput de, no mínimo, 800 (oitocentos) Mbps com a funcionalidade de Threat Prevention, ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Antivírus habilitadas;

15.2.4. Throughput de, no mínimo, 6 (seis) Gbps de VPN IPSec;

15.2.5. Estar licenciada para ou suportar sem o uso de licença de, no mínimo, 200 (duzentos) clientes de VPN SSL simultâneos;

15.2.6. Estar licenciado para, ou suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos

15.2.7. Suportar no mínimo 700 (setecentos) Mbps de throughput de Inspeção SSL;

15.2.8. Suporte a, no mínimo, 1.400.000 (um milhão quatrocentos mil) conexões simultâneas;

15.2.9. Suporte a, no mínimo, 42.000 (quarenta e duas mil) novas conexões por segundo;

15.2.10. Possuir ao menos 5 (cinco) interfaces de 1GbE RJ45, sendo pelo menos 1 dela utilizada para gerenciamento;

15.2.11. Possuir pelo menos 2 (duas) interfaces 1GbE SFP e seus módulos. Deverão ser fornecidos com 2 (dois) transceivers;

15.2.12. Possuir pelo menos 1 (uma) interface do tipo console

15.2.13. Suporte a, no mínimo, 15 (quinze) zonas de segurança;

15.2.14. Possuir armazenamento de no mínimo 120 (cento e vinte) GB SSD;

15.2.15. Fonte de alimentação interna ou externa, que opere com ajuste automático de tensão 110-220 Volts;

15.2.16. Deve suportar a instalação em rack padrão 19” ou ser entregue com bandeja para a instalação em rack padrão 19”;

CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE FIREWALL

15.2.17. É permitida a composição da solução ofertada dentro do mesmo fabricante, sendo vedada solução de software livre;

15.2.18. A solução devera ser compatível com SMPv2 e SMPv3;

15.2.19. Os Appliances devem permitir acesso ao equipamento via interface de linha de comando (CLI), console, SSH além de interface web HTTPS;

15.2.20. Devem ser capazes de criptografar e autenticar a comunicação com a solução de gerenciamento centralizado e/ou de orquestração;

15.2.21. Devem ser capazes de bloquear sessões TCP que utilizarem variações do 3-way handshake, como 4-way e 5-way split handshake, de modo a prevenir possíveis tráfegos maliciosos;

15.2.22. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos do mesmo fabricante, desde que obedeçam a todos os requisitos desta especificação;

15.2.23. A comunicação entre os appliances de segurança e o módulo de gerência deve ser por meio criptografado;

15.2.24. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

15.2.25. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior data da proposta;

15.2.26. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

15.2.27. A solução deve suportar a possibilidade de manutenção dinâmica de um equipamento de um cluster para outro, de acordo com a necessidade da arquitetura definida, sem que haja a perda do tráfego;

15.2.28. A solução de balanceamento deverá ser fornecida em appliances físicos.

15.2.29. A solução de balanceamento deverá ser fornecida em Alta Disponibilidade do tipo Ativo/Ativo;

15.2.30. Os appliances deverão vir acompanhados de todos os conectores, cabeamento e peças de fixação no Rack, necessários à sua instalação e funcionamento, conforme as especificações deste Estudo Técnico Preliminar.

15.2.31. Deve prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

15.2.32. A solução deverá ser provida de forma redundante, de modo que se houver a falha de uma delas, a outra possa assumir totalmente o controle, sem que haja perda do tráfego;

15.2.33. A solução deverá ser capaz de organizar os appliances de NG Firewall em grupos de segurança, nos quais os appliances de NG Firewall atuarão com seus recursos somados;

15.2.34. A solução deverá ser capaz de suportar, no mínimo, 4 (quatro) grupos de segurança;

15.2.35. A solução deverá possuir a quantidade de transceptores suficientes para conectar toda a solução à rede corporativa, o que inclui a gerência.

REQUISITOS GERAIS DE SOFTWARE

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

15.2.37. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

15.2.38. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM, IGMP), DHCP Relay, DHCP Server e Jumbo Frames;

15.2.39. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

15.2.40. Deve suportar, no mínimo, roteamento BGP, OSPFv2, RIPv2 e roteamento estático;

15.2.41. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

15.2.42. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

15.2.43. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server no protocolo IPv6;

15.2.44. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

15.2.45. Deve suportar NAT dinâmico (Many-to-Many);

15.2.46. Deve suportar NAT estático (1-to-1);

15.2.47. Deve suportar NAT estático bidirecional 1-to-1;

15.2.48. Deve suportar Tradução de porta (PAT);

15.2.49. Deve suportar NAT de Origem;

15.2.50. Deve suportar NAT de Destino;

15.2.51. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

15.2.52. Deve implementar Network Prefix Translation (NPTv6) ou NAT66 (IPv6-to-IPv6), prevenindo problemas de roteamento assimétrico;

15.2.53. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco e situação do cluster;

15.2.54. Enviar log para sistemas de monitoração externos;

15.2.55. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

15.2.56. Proteção anti-spoofing;

15.2.57. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

15.2.58. Suporte a configuração de alta disponibilidade (HA) Ativo/Passivo e Ativo/Ativo. Caso o suporte à configuração de alta disponibilidade (HA) implique em algum licenciamento adicional que aumente o valor da proposta esta funcionalidade não deverá ser incluída nos equipamentos do Grupo II;

15.2.59. A configuração em alta disponibilidade (HA) deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;

15.2.60. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

15.2.61. Suportar cluster para alta-disponibilidade do tipo ativo-ativo, permitindo que um cluster possa realizar o load balance das sessões para inspeção profunda sem a necessidade de implementações ou mudanças na rede ou nos terminais já existentes;

15.2.62. Controle, inspeção e descriptografia de SSL para tráfego de Saída (Outbound);

15.2.63. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

15.2.64. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. 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.

POLÍTICAS

15.2.65. Deverá suportar controles por zonas de segurança;

15.2.66. Deverá suportar controles de políticas por porta e protocolo;

15.2.67. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

15.2.68. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

15.2.69. Controle de políticas por nome ou código de País (Por exemplo: BR, US, UK, RU);3.1.7.6. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

15.2.70. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

15.2.71. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

15.2.72. Suporte a objetos e regras IPV6;

15.2.73. Suporte a objetos e regras multicast;

15.2.74. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários e datas pré-definidos automaticamente.

CONTROLE DE APLICAÇÕES

15.2.75. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

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

15.2.77. Reconhecer pelo menos 3.000 (três mil) aplicações diferentes, incluindo, mas não limitado: a 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;

15.2.78. 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, onedrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

15.2.79. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
3.1.8.6. 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 utilização da rede Tor;

15.2.80. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

15.2.81. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

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

15.2.83. Atualizar a base de assinaturas de aplicações automaticamente;

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

15.2.85. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

15.2.86. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

15.2.87. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

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

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

15.2.90. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

15.2.91. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts,Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

15.2.92. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;

15.2.93. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

15.2.94. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (ClientServer, Browse Based, Network Protocol, etc);

15.2.95. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;

15.2.96. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

PREVENÇÃO DE AMEAÇAS

15.2.97. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

15.2.98. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

15.2.99. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

15.2.100. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: Permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

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

15.2.102. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

15.2.103. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

15.2.104. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

15.2.105. Deve permitir o bloqueio de vulnerabilidades;

15.2.106. Deve permitir o bloqueio de exploits conhecidos;

15.2.107. Deve incluir proteção contra-ataques de negação de serviços;

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

15.2.109. Detectar e bloquear a origem de portscans;

15.2.110. Bloquear ataques efetuados por worms conhecidos;

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

15.2.112. Possuir assinaturas para bloqueio de ataques de buffer overflow;

15.2.113. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

15.2.114. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

15.2.115. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMTP e POP3;

15.2.116. Identificar e bloquear comunicação com botnets;

15.2.117. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

15.2.118. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

15.2.119. Os eventos devem identificar o país de onde partiu a ameaça;

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

15.2.121. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

15.2.122. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários,origem, destino, zonas de segurança, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

15.2.123. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

15.2.124. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

15.2.125. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

FILTRO DE URLS

15.2.126. 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);

15.2.127. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

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

15.2.129. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

15.2.130. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

15.2.131. Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;

15.2.132. Possuir pelo menos 70 categorias de URLs;

15.2.133. Deve possuir a função de exclusão de URLs do bloqueio;

15.2.134. Permitir a customização de página de bloqueio;

15.2.135. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

IDENTIFICAÇÃO DE USUÁRIOS

15.2.136. 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;

15.2.137. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

15.2.138. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2018;

15.2.139. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

15.2.140. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

15.2.141. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

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

15.2.143. 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;

15.2.144. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

15.2.145. Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);

15.2.146. A solução deve suportar nativamente a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X;

FILTRO DE DADOS

15.2.147. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

15.2.148. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

15.2.149. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

15.2.150. 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.

GEOLOCALIZAÇÃO

15.2.151. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

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

VPN

15.2.153. Suportar VPN IPSec Site-to-Site;

15.2.154. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

15.2.155. A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

15.2.156. A VPN IPSEc deve suportar no mínimo Diffie-Hellman Group 1, Group 2, Group 5;

15.2.157. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

15.2.158. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

15.2.159. Deve possuir integração com Amazon, AWS, Google Cloud, IBM Cloud VPC, Kubernetes, Azure a fim de permitir a criação de objetos dinâmicos com base nos endereços IPs das instancias virtuais na nuvem;

15.2.160. O cliente VPN deve suportar autenticação via SAML 2.0 a fim de permitir integração com plataformas Azure AD, Google Authentication ou outro provedor de identidade;

15.2.161. O cliente de VPN deve estar disponível na loja de aplicativos AppStore e PlayStore;

SD-WAN

15.2.162. 3.1.15.1. Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação;

15.2.163. As funcionalidades de segurança e SD-WAN que compõem a solução devem funcionar em equipamento único obedecendo a todos os requisitos desta especificação;

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

15.2.165. Deve ser possível criar políticas para modelagem do tráfego definido pelo menos os parâmetros:

15.2.166. IP de origem;

15.2.167. Grupo de usuário

15.2.168. VLAN de origem;

15.2.169. IP de destino;

15.2.170. Porta TCP/UDP de destino;

15.2.171. Domínio e URL de destino;

15.2.172. Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox);

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

15.2.174. O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

15.2.175. O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade e realizar a reordenação dos pacotes desse mesmo fluxo no outro extremo;

15.2.176. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

15.2.177. A solução deve permitir a definição do roteamento para cada aplicação;

15.2.178. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis mínimos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

15.2.179. Deve possibilitar a definição do link de saída para uma aplicação específica;

15.2.180. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, dois links;

15.2.181. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

15.2.182. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;

15.2.183. Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);

15.2.184. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

15.2.185. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;

15.2.186. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;

15.2.187. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:

15.2.188. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

DAS FUNCIONALIDADES DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

15.2.189. A solução devera contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

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

15.2.191. Deve de-criptografar trafego de entrada e saída em conexões negociadas com TLS 1.2;

15.2.192. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

15.2.193. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

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

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

15.2.196. Reconhecer pelo menos 3.000 (Três mil) aplicações diferentes, incluindo, mas não limitado: a trafego 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;

15.2.197. Para trafego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

15.2.198. A solução deve suportar a recategorização de URLs local;

15.2.199. Atualizar a base de assinaturas de aplicações automaticamente;

15.2.200. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;

15.2.201. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDCP/CD;

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

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

15.2.204. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

15.2.205. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

15.2.206. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

15.2.207. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

15.2.208. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

15.2.209. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

15.2.210. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

15.2.211. Suportar a criação de categorias de URLs customizadas;

15.2.212. Permitir a customização de pagina de bloqueio;

15.2.213. Como melhor prática do uso do acesso a internet e respeitando as políticas de segurança do orgão, a ferramenta deve criar uma página customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma pagina URL ou aplicação WEB de acordo com as políticas de acesso estabelecidas pela área de TI;

15.2.214. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

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

15.2.216. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos:

15.2.217. PCI – números de cartão de crédito;

15.2.218. Arquivos PDF;

15.2.219. Arquivos executáveis;

15.2.220. Arquivos de banco de dados;

15.2.221. Arquivos do tipo documento;

15.2.222. Arquivos do tipo apresentação;

15.2.223. Arquivos do tipo planilha;

15.2.224. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload";

15.2.225. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma pagina web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito;

15.2.226. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes sendo trafegados pela Web em paginas utilizando o protocolo HTTPS.

DAS FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

15.2.227. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti- Malware integrados no próprio equipamento de firewall;

15.2.228. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

15.2.229. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

15.2.230. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

15.2.231. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

15.2.232. A solução de IPS deve possuir análise de padrões de estado de conexões, analise de decodificação de protocolo, analise para detecção de anomalias de protocolo, remontagem de pacotes de TIP e bloqueio de pacotes malformados;

15.2.233. Detectar e bloquear a origem de portscans;

15.2.234. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

15.2.235. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;

15.2.236. Possuir assinaturas para bloqueio de ataques de buffer overflow;

15.2.237. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

15.2.238. Suportar bloqueio de arquivos por tipo;

15.2.239. Identificar e bloquear comunicação com botnets;

15.2.240. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

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

15.2.242. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e AntiMalware, através da console de gerência centralizada;

15.2.243. Os eventos devem identificar o país de onde partiu a ameaça;

15.2.244. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

15.2.245. Possuir a capacidade de prevenção de ameaças não conhecidas;

15.2.246. Suportar a criação de políticas por Geo-Localização, permitindo que o trafego de determinado País/Países seja bloqueado;

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

15.2.248. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

DAS FUNCIONALIDADES E CONTROLE DE QUALIDADE DE SERVIÇO

15.2.249. Suportar a criação de políticas de QoS por:

15.2.250. Endereço de origem, endereço de destino e por porta;

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

15.2.252. Banda garantida;

15.2.253. Banda máxima ;

15.2.254. Fila de prioridade;

15.2.255. Disponibilizar estatísticas RealTime para classes de QoS;

DAS FUNCIONALIDADES DE VPN

15.2.256. Suportar VPN Site-to-Site e Cliente-To-Site;

15.2.257. Suportar IPSec VPN;

15.2.258. 4.8.7.3. Suportar SSL VPN;

15.2.259. A VPN IPSEc deve suportar:

15.2.260. 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

15.2.261. A solução deve suportar CA Interna e CA Externa de terceiros;

15.2.262. A Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

GERENCIAMENTO CENTRALIZADO DE LOGS E RELATÓRIOS - ITEM 3

15.2.263. Os equipamentos devem ser mantidos atualizados na última versão de sistema operacional disponível pelo fabricante durante o período de vigência contratual;

15.2.264. Os equipamentos devem ser do mesmo fabricante da solução de firewall;

15.2.265. Deve fornecer throughput mínimo de 25 GB/dia de Logs;

15.2.266. Deve possuir capacidade de armazenamento de no mínimo 10TB;

15.2.267. Deve possibilitar o envio/backup dos logs para um servidor de logs;

15.2.268. Monitorar todo o tráfego e atividade da rede de dados da SSPDF, inclusive o tráfego e comunicação com a internet e redes externas;

15.2.269. Apresentar histórico e fornecer relatórios das atividades realizadas na administração e operação da solução, bem como de todo o tráfego controlado e monitorado pela mesma;

15.2.270. Deve permitir relatórios customizados na solução;

15.2.271. Deve permitir geração de relatórios agendados ou sob demanda;

15.2.272. Deve possuir relatórios pré-definidos na solução;

15.2.273. Deve possuir console única de gerenciamento;

15.2.274. Suporte a hypervisor VMware ESX/ESXi 5.5/6.0/6.5/6.7/7.0, no mínimo.

GRUPO 2 (ITENS 4 e 5)

DA SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS - EDR

15.2.275. A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo CPT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa análise executada na nuvem proprietária da próprio fabricante ou appliance dedicada para sandboxing;

15.2.276. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTC durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente;

15.2.277. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

15.2.278. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

15.2.279. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

15.2.280. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTC) e Mirror/TAP;

15.2.281. A tecnologia de máquina virtual devera possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas;

15.2.282. A solução de prevenção de ameaças avançadas (Sandboxing) contra ataques persistentes e ZeroDay, deve ser habilitada e funcionar de forma independente, ou seja, não sendo obrigatório o uso e ativação de funcionalidades ou engines de anti-vírus para a mesma ter o seu devido funcionamento;

15.2.283. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

15.2.284. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb;

15.2.285. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

15.2.286. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. a solução deve permitir a analise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm;

15.2.287. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

15.2.288. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

15.2.289. Quantidade de arquivos que estão em emulação;

15.2.290. Número de arquivos emulados;

15.2.291. A solução deve possuir os indicadores abaixo referente ao ultimo dia, ultima semana ou últimos 30 dias:

15.2.292. Arquivos scaneados;

15.2.293. Arquivos maliciosos;

SOLUÇÃO EDR

15.2.294. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação:

15.2.294.1. No mínimo, 2 interfaces 1000Base-T com conectores RJ-45;

15.2.294.2. Discos redundantes com espaço de armazenamento para LOGs de pelo menos 8TB;

15.2.294.3. Possuir fonte de energia AC redundante com ajuste automático de tensão para operação nas tensões de 100 a 240-VAC/60 Hz;

15.2.294.4. Ser fornecido com todos os acessórios necessários para sua instalação.

15.3. **SOLUÇÃO DE ANTIVÍRUS – LICENÇA PERPÉTUA**

15.3.1. Características gerais antivírus para estações de trabalho e servidores:

15.3.2. Entende-se por agente ou antivírus como sendo a ferramenta de proteção contra malwares ou vírus, termo a ser usado tanto para os componentes de proteção de estações de trabalho ou equipamentos servidores;

15.3.3. A Solução deverá ser baseada na arquitetura cliente/servidor, sendo composta por componente de gerência centralizada e agentes antivírus:

15.3.4. O serviço de gerência centralizada deverá ser onpremise, essa deverá ser disponibilizada por meio de appliance virtual do mesmo fabricante da solução ofertada ou a Contratada deverá realizar a instalação e configuração do(s) servidor(es) no ambiente disponibilizado, sem custo adicional para o Contratante;

15.3.5. O tráfego de dados entre os agentes e gerência centralizada deverá ocorrer através de conexão segura;

15.3.6. Os componentes da solução deverão manter compatibilidade com o ambiente tecnológico da SSPDF;

15.3.7. A solução deverá permitir instalação dos agentes de forma remota, por meio de GPO do Windows abrangendo todas as Seções e Subseções;

15.3.8. A solução deverá ser fornecida pronta para utilização imediata, não sendo permitida apresentação de qualquer procedimento que configure o desenvolvimento da solução após a contratação;

15.3.9. A solução deverá ser de um único fabricante, não devendo ser composta por módulos, softwares, scripts ou plug-ins de terceiros;

15.3.10. Ressalvados os casos em que a solução ofertada utilize módulos do próprio Sistema Operacional, como Firewall e recursos de proteção antimalware nativos;

15.3.11. A solução deverá oferecer proteção em camadas para detecção de malwares;

15.3.12. O fabricante deverá oferecer serviço de análise e criação de solução específica para quando for identificado um possível malware não detectado pela solução antivírus;

15.3.13. Entende-se por licença perpétua aquela que após o encerramento do contrato de suporte firmado pela administração publica, permanecerá funcionando, até que o fabricante informe que as licenças não receberão suporte e atualização, permanecendo com as antigas atualizações.

GERENCIAMENTO CENTRALIZADO

15.3.14. A console de gerência centralizada deverá oferecer interface baseada em modo gráfico (GUI) acessível por software ou navegador web de forma segura (HTTPS);

15.3.15. Permitir o gerenciamento, controle, configuração e operação de todo parque (produtos instalados nos clientes e quaisquer outros módulos que componham a solução) de forma remota e centralizada;

15.3.16. A gerência centralizada deverá estar em consonância e compatibilidade com o ambiente tecnológico exposto no item 04 deste Anexo;

15.3.17. Deverá permitir acessos simultâneos de vários usuários à console da gerência (sessões);

15.3.18. Deverá possuir uma base de dados centralizada para armazenamento das informações e logs dos clientes e da gerência;

15.3.19. Deverá permitir a criação e distribuição de políticas e tarefas remotamente para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência;

15.3.20. Deverá permitir operações de instalação, desinstalação e atualização dos módulos da solução para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência ou de GPO do Windows;

15.3.21. Oferecer mecanismo de comunicação (via push) entre o(s) servidor(es) e os clientes para entrega de dados e informações;

15.3.22. Oferecer mecanismo de comunicação (via pull) entre os clientes e o(s) servidor(es) para consulta de dados e informações;

15.3.23. A instalação ou atualização dos módulos componentes da solução, distribuição de configurações, políticas e tarefas da gerência aos clientes deve ser realizada de forma silenciosa e sem necessidade de reinicialização ou logoff do equipamento e sem necessidades de aguardar alguma ação do usuário do equipamento;

15.3.24. Deverá oferecer funcionalidade de execução, criação e customização de consultas às informações contidas na base de dados;

15.3.25. Deverá possibilitar a disponibilização das informações em modo de gráficos ou tabelas;

15.3.26. Deverá ser possível exportar as informações obtidas nas consultas em pelo menos um desses formatos: PDF, HTML, TXT, CSV ou Json;

15.3.27. Deverá permitir criação de alertas e notificação de eventos para administradores e usuários determinados;

15.3.28. Deverá possibilitar pesquisa no histórico de eventos;

15.3.29. Deverá permitir execução de consultas por agendamento e envio do resultado via email;

15.3.30. Deverá disponibilizar as seguintes consultas pré-definidas:

15.3.30.1. Máquinas com maior número de ocorrência de vírus e ameaças;

15.3.30.2. Usuários com maior número de ocorrência de vírus e ameaças;

15.3.30.3. Histórico de infecções nas últimas 24 horas, 7 dias e 30 dias;

15.3.30.4. Vírus e ameaças com maior número de registros nas últimas 24 horas, 7 dias e 30 dias;

15.3.30.5. Versões dos produtos instalados;

15.3.30.6. Versões das vacinas, quando for o caso, ou outras políticas de proteção adotadas.

15.3.31. Deverá permitir criação de dashboards;

15.3.32. Deverá permitir integração com o Active Directory da SSPDF para descoberta de equipamentos ou de forma nativa na própria solução;

15.3.33. Deverá dar suporte a estrutura de florestas/domínios e subdomínios do Active Directory, refletindo a estrutura hierárquica da SSPDF no Active Directory:

15.3.34. Deverá ser capaz de distinguir e agrupar equipamentos servidores, estações de trabalho e notebooks, de forma a definir agrupamentos distintos para aplicação de regras, tarefas e políticas;

15.3.35. Deverá permitir que se configure diferentes políticas e tarefas para diferentes agrupamentos de computadores, seja para pontos específicos na estrutura em árvore (Seção, Subseção) como para demais grupos específicos (servidores ou estações de trabalho);

15.3.36. Deverá possibilitar função de herança de políticas e tarefas entre os grupos e subgrupos, com possibilidade de quebra de herança;

15.3.37. O acesso à console da gerência centralizada deverá ser efetuado mediante autenticação segura através de usuário cadastrado na base de dados da solução ou através de autenticação integrada com usuários do Active Directory;

15.3.38. Todas as ações realizadas pelos usuários da gerência deverão ser registradas em log de auditoria, com no mínimo descrição da ação, nome do usuário, data e hora da ação realizada:

15.3.38.1. Deve permitir cadastro de usuários com, pelo menos, os seguintes perfis (ou equivalentes):

15.3.38.2. Administradores, com acesso a todas as funcionalidades da gerência e em toda a estrutura hierárquica da SSPDF;

15.3.38.3. Administradores locais, com acesso a funcionalidades específicas e em pontos de domínios específicos da estrutura hierárquica da SSPDF;

15.3.38.4. Visualização ou monitoramento, podendo abranger todo contexto da estrutura hierárquica da SSPDF ou pontos específicos;

15.3.39. Deverá permitir instalação e desinstalação remota dos agentes antivírus, através da console de gerenciamento ou de GPO do Windows;

15.3.40. A solução deverá ser capaz de detectar e listar equipamentos conectados na rede e que não possuam a solução instalada;

15.3.41. Deverá identificar através da integração com o Active Directory, ou de forma nativa pela própria solução, computadores sem o agente antivírus instalado;

15.3.42. Deverá apresentar a funcionalidade de instalação da solução nos equipamentos detectados através da listagem de equipamentos sem o antivírus instalado ou por meio do Active Directory ou por orquestradores.

15.3.43. Deverá possibilitar o download de pacotes executáveis de instalação para proceder com instalação manual nos equipamentos, observado os sistemas operacionais suportados;

15.3.44. Deverá permitir limpeza automática de agentes inativos por determinado período de tempo, liberando as respectivas licenças;

15.3.45. Deverá ser possível criação de políticas para distribuição de atualizações para o parque gerenciado com periodicidade mínima diária;

15.3.46. Deverá ser possível criação de políticas para distribuição de atualizações e vacinas para o parque gerenciado com periodicidade mínima diária;

15.3.47. Deverá permitir configuração alternativa para permitir que o agente busque atualização na nuvem do fabricante quando estiver fora do escopo da gerência centralizada;

15.3.48. As atualizações deverão ser do tipo incremental;

15.3.49. Deverá permitir distribuição de versões diferentes da solução para diferentes grupos de equipamentos;

15.3.50. Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, restaurar e excluir;

15.3.51. Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, limpar e excluir;

15.3.52. Deverá possibilitar restauração manual de arquivos quarentenados;

15.3.53. Deverá permitir criar listas de exclusões ou exceções para determinados aplicativos ou diretórios e subdiretórios;

15.3.54. Deverá utilizar os recursos locais de forma otimizada, sem impacto no desempenho do endpoint, ou possibilitar a configuração de baixo uso de recurso do dispositivo nas operações do agente antivírus;

15.3.55. Deverá permitir criação de políticas para bloqueio de dispositivos de armazenamento externos;

15.3.56. Deverá possibilitar extração de informações sobre dispositivos bloqueados, contendo no mínimo data e hora do ocorrido, equipamento onde o bloqueio ocorreu, rótulo do dispositivo bloqueado e usuário do sistema operacional logado durante o bloqueio;

15.3.57. Deverá fornecer solução Sandbox, on-premise, para análise de malwares e mecanismo de reputação de softwares.

15.3.57.1. Em caso de fornecimento do Sandbox on-premise a Contratada deverá instalar e fornecer todos os recursos logísticos e de infraestrutura necessários para implantação do equipamento no ambiente do Contratante, a exemplo de alimentação elétrica, cabeamento, sem custo adicional.

15.3.57.2. As funcionalidades do serviço de Sandbox deverão ser integrados na gerência centralizada;

15.3.57.3. Deverá possibilitar aplicar bloqueios e respostas para ameaças detectadas e analisadas pelo serviço de Sandbox em todo o parque;

15.3.57.4. Deverá apresentar interface para investigação usando funcionalidades de Detecção e Resposta, sendo possível tomar ações para os equipamentos em análise;

SERVIÇO DE DESINSTALAÇÃO

15.3.58. A desinstalação do parque atual existente na SSPDF deverá ser efetuada pela CONTRATADA;A CONTRATANTE deverá fornecer as credenciais necessárias para a execução da desinstalação, como usuário com privilégio.

15.3.59. A estratégia a ser adotada na execução da desinstalação será previamente acordada entre o CONTRATANTE e a CONTRATADA.

15.3.60. A desinstalação da ferramenta existente deverá ocorrer de forma silenciosa para o usuário;

15.3.60.1. Em casos específicos onde seja necessário reboot, deverá ser informado para a CONTRANTE para que se monte uma estratégia de forma a não interromper o fluxo de trabalho onde se necessitar;

15.3.61. O equipamento onde for instalado a nova solução deverá estar LIMPA e sem vestígios da instalação anterior, de forma que não se acarrete crashes e erros na instalação do novo agente e que não ocorra situações em que mais de 1 solução além da vigente por este certame estejam instaladas no equipamento ao mesmo tempo;

15.3.62. Problemas na execução da desinstalação do agente deverão ser imediatamente comunicadas a CONTRATANTE;

SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

15.3.63. A instalação deverá ocorrer em todo o âmbito da SSPDF;

15.3.64. A instalação do agente deverá pressupor desinstalação da solução anterior;

15.3.65. A instalação do agente deverá ser imperceptível para o usuário, de forma a não aparecer pop-ups, mensagens, caixas de diálogos solicitando ação de usuário e nem janelas modais, de forma a interromper de qualquer forma o usuário;

15.3.66. Os serviços de instalação devem compreender a configuração da gerência centralizada em servidores virtuais para os componentes da solução on-premise, incluindo appliance virtual da gerência centralizada, banco de dados da solução e demais componentes a serem utilizados pela solução de gerência;

15.3.67. Deverá possibilitar a instalação dos componentes da solução de forma a refletir a estrutura hierárquica da SSPDF,

15.3.68. A instalação dos agentes deverá ser realizada de forma remota, abrangendo todas as Seções e Subseções;

15.3.69. Deve permitir que se instale os agentes individualmente por computador ou em lote, para vários computadores;

15.3.70. A interoperabilidade entre os componentes da solução deverá ser configurada por políticas na gerência e utilizando protocolos seguros;

15.3.71. Deverá permitir que se programe através de políticas o agendamento da distribuição dos itens atualizados na gerência centralizada para os repositórios;

15.3.72. Ao final do processo de instalação a CONTRATADA deverá fornecer os seguintes relatórios:

15.3.72.1. Relação de todos os computadores contendo antivírus instalado, com no mínimo as seguintes informações, agrupados por localidade

15.3.72.2. Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subsecretaria/SSPDF, contendo no mínimo:

15.3.72.3. Versão de cada módulo da solução instalado;

15.3.72.4. Versão da DAT, catálogo ou relatório de vacinas instaladas no endpoint;

15.3.72.5. Versão de demais bibliotecas ou catálogos que compõem a solução instalado;

15.3.72.6. Os relatórios serão utilizados para avaliar conformidade da prestação do serviço de instalação;

15.3.72.7. Serão comparados com o quantitativo de máquinas ativas na SSPDF, utilizando a seguinte fórmula para apurar o índice de instalação:

a) IND – Índice de instalação;

b) QAI – Quantidade de computadores com antivírus instalado;

c) QLA – Quantidade licenças adquiridas;

d) Será dado aceite da solução quando o resultado da instalação IND possua valor igual ou superior a 0.8 – IND >= 0.8;

SOLUÇÃO DE ANTIVÍRUS PARA ESTAÇÕES DE TRABALHO

15.3.73. Deverá ser compatível com as seguintes tecnologias de sistema operacional, no mínimo:

15.3.73.1. Windows 10;

15.3.73.2. Windows 11;

15.3.74. Deverá proporcionar proteção contra ameaças, tais como vírus, ransomwares, trojans, spywares, worms, keylogers, dentre outros malwares;

15.3.75. A solução e todos os seus componentes deverão funcionar como um agente composto por um executável que será instalado na estação de trabalho, podendo encapsular os diversos módulos que compõe a solução;

15.3.75.1. Caso a solução utilize de recursos de segurança nativos do Sistema Operacional, os mesmos serão considerados como módulos do agente único utilizado;

15.3.75.2. O módulo EDR poderá ser disponibilizado através de um executável ou módulo separado ao da solução de antivírus;

15.3.76. Deverá ser capaz de reconhecer ataques e ações maliciosas por assinatura, por análise heurística ou por machine learning;

15.3.77. Soluções que usem somente método de detecção por assinatura não serão aceitas;

15.3.78. Deverá possuir mecanismo de análise comportamental;

15.3.79. Deverá ser capaz de proteger ataques provenientes de malwares;

15.3.80. Deverá ser capaz de realizar proteção contra ameaças mesmo estando o dispositivo não conectado à internet;

15.3.81. Quando o equipamento estiver fora da cobertura da gerência centralizada deverá ser capaz de buscar atualizações na internet, na nuvem do fabricante;

15.3.82. Deverá permitir criar bloqueios personalizados, baseado no nome do aplicativo, caminho do aplicativo e hash do arquivo;

15.3.83. Deverá ser capaz de detectar, alertar e prevenir quando for detectado alguma ameaça;

15.3.84. Deverá ser capaz de prover proteção contra-ataques que explorem vulnerabilidades do sistema operacional do host, de acordo com o estabelecido no item 2.18.1 deste Anexo;

15.3.85. Deverá possuir proteção contra BOTs e variantes;

15.3.86. Deverá efetuar proteção permanente e em tempo real dos processos em memória;

15.3.86.1. Processos suspeitos deverão ser bloqueados;

15.3.87. Deverá possuir mecanismos de análise avançada para proteção e remediação de vírus de código polimorfos, ofuscados, criptografados e contra ameaças avançadas e persistentes, que não são detectadas pelos métodos convencionais de antivírus;

15.3.88. Deverá ser capaz de detectar variações de malwares geradas em memória principal;

15.3.89. Deverá oferecer tecnologia de proteção baseada em técnicas de Inteligência Artificial do tipo Machine Learning;

15.3.90. Em casos de aplicações com comportamento malicioso detectado, deverá efetuar bloqueios de processos e efetuar isolamento de comunicação;

15.3.91. Deverá oferecer proteção contra-ataques de 0Day (dia zero);

15.3.92. Deverá oferecer proteção contra Ransomwares, com capacidade de avaliar processos criptográficos em execução no sistema, exclusão de backups, número alto de operações de I/O no sistema de arquivos;

15.3.93. Deverá informar o nome ou endereço IP da origem do ataque ou infecção;

15.3.94. Deverá oferecer funcionalidade de controle de aplicações, identificando aplicações no mínimo pelo código Hash do executável, caminho e nome do aplicativo malicioso;

15.3.95. Deverá oferecer proteção contra vírus de macro e por scripts variados, incluindo bash e powershell;

15.3.96. Deverá oferecer mecanismo de bloqueio baseado em análise realizada pela central de inteligência do fabricante oriundo da nuvem;

15.3.97. Deverá implementar técnicas de Detecção e Resposta (EDR) para prover detecção e investigação para atividades suspeitas;

15.3.98. Deverá possibilitar visualizar toda a cadeia de ataque, inclusive os processos e aplicativos executados, arquivos e registros utilizados, endereços acessados, dentre outros;

15.3.99. Deverá oferecer proteção para alterações suspeitas de registro;

15.3.100. Deverá prover mecanismos para criação proteções personalizadas para detecção;

15.3.101. Deverá oferecer proteção contra processos que tentem alterar ou manipular indevidamente os componentes instalados e em execução do antivírus (autoproteção);

15.3.102. Deverá oferecer proteção contra-ataques direcionados;

15.3.103. Deverá gerar log local assim como enviá-los para a gerência;

15.3.104. Deverá permitir inclusão de exceções aplicações e caminhos;

15.3.105. A solução deverá oferecer proteção para ameaças em execução:

15.3.105.1. Na memória principal (RAM);

15.3.105.2. Em arquivos;

15.3.105.3. No tráfego de rede;

15.3.105.4. Em dados provenientes de browsers de navegação web (downloads, scripts, etc);

15.3.105.5. Em arquivos compactados (formatos zip, exe, cab, rar, etc);

15.3.105.6. Em processos de inicialização automática;

15.3.105.7. Em serviços criados/modificados;

15.3.106. Solução deverá efetuar a proteção permanente, em tempo real, quando arquivos forem acessados, lidos, gravados, alterados ou renomeados;

15.3.107. Deverá permitir bloqueio de alterações nas configurações do antivírus por parte do usuário, sendo permitido apenas por alterações de políticas ou mediante inserção de senha/password, definidos na gerência;

15.3.108. Deverá possibilitar a criação de lista de aplicações confiáveis (lista de exceções), a partir da gerência centralizada, para eliminação de detecções do tipo falso positivo;

15.3.109. Deverá oferecer a possibilidade de editar esta lista, com inclusão e remoção de aplicativos;

15.3.110. Deverá possuir a capacidade de detectar antivírus de outros fabricantes que possam acarretar incompatibilidade;

15.3.111. Deverá impedir execução e instalação de aplicativos cujo comportamento seja suspeito ou que constem na lista de aplicativos inseridos na gerência centralizada;

15.3.112. Deverá detectar e proteger em tempo real o computador contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de páginas da web e scripts em linguagens tais como javascript, vbscript, activex, etc;

15.3.113. Deverá oferecer mecanismo de controle de dispositivos externos;

15.3.114. A administração das regras da funcionalidade para controle mecanismos externos deverá ser realizada a partir da gerência centralizada;

15.3.115. O mecanismo de controle de dispositivos externos deverá possibilitar monitorar e bloquear dispositivos a partir de regras e políticas estabelecidas na gerencia centralizada, para no mínimo:

15.3.116. Dispositivos de rede externos (wifi portátil, dispositivos de dados móveis);

15.3.117. Transferências de dados para dispositivos mobile.;

15.3.118. Transferências de dados para dispositivos de armazenamento externos;

15.3.119. Possibilitar ações de bloqueio na execução de arquivos em transferência através de browsers e clientes de e-mail.

15.3.120. Deve oferecer ou executar uma das seguintes opções de ações corretivas para programas maliciosos detectados: bloquear o objeto, executar a limpeza da ameaça e executar ação de quarentena;

15.3.121. Os mecanismos de proteção deverão ser executados sem comprometer o desempenho dos computadores, de forma que não seja perceptível aos seus usuários e nem influenciem negativamente no rendimento de aplicações em servidores;

15.3.122. No mínimo as seguintes ocorrências deverão ser registradas em arquivo de log local ou enviadas para a gerência centralizada:

15.3.122.1. Atualização de engine e/ou repositório de vacinas.

15.3.122.2. Recebimento de políticas e tarefas da gerência;

15.3.122.3. Inicialização e finalização de varreduras, agendadas ou manuais, ou quando realizada por meio de análise dos processos em tempo real baseado em machine learning;

15.3.122.4. Detecção de alguma ameaça, registrando no mínimo as seguintes informações:

a) Nome da ameaça;

b) Tipo da ameaça;

c) Arquivo ou local infectado;

d) Data e hora da detecção;

e) Mecanismo que gerou a detecção;

f) Nome da máquina/endereço IP;

g) Ação realizada;

h) Usuário logado no sistema;

15.3.123. Deverá buscar por itens de atualização nos repositórios, configurado pela gerência, de acordo com topologia e políticas especificadas;

15.3.124. Deverá possibilitar mais de uma versão da ferramenta e seus insumos, para que em casos de incompatibilidades decorrentes de atualizações, seja possível reinstalar versões anteriores estáveis ou instalar versões novas em grupos específicos, para fins de testes de compatibilidade antes de instalação em todo parque;

15.3.125. Deverá fornecer informações do status do agente e de seus componentes, através da gerência com informações atualizadas com delay máximo de 5 minutos;

15.3.126. Deve ser disponibilizado nos idiomas português, preferencialmente, ou inglês;

15.4. **SOLUÇÃO DE ANTIVÍRUS PARA EQUIPAMENTOS SERVIDORES**

15.4.1. Deverá ser compatível com as seguintes tecnologias de sistema operacional, no mínimo:

15.4.1.1. Windows Server 2008 R2;

15.4.1.2. Windows Server 2012;

15.4.1.3. Windows Server 2016;

15.4.1.4. Windows Server 2019 e posteriores;

15.4.1.5. VMware ESXi;

15.4.1.6. Deverá proporcionar proteção contra ameaças, tais como vírus, ransomwares, trojans, spywares, worms, keylogers, dentre outros malwares;

15.4.1.7. A solução e todos os seus componentes deverão funcionar como um agente composto por um executável único que será instalado na estação de trabalho, podendo encapsular os diversos módulos que compõe a solução;

15.4.2. Caso a solução utilize de recursos de segurança nativos do Sistema Operacional, os mesmos serão considerados como módulos do agente único utilizado;

15.4.3. Deverá ser capaz de reconhecer ataques e ações maliciosas por assinatura, por análise heurística ou por machine learning.

15.4.4. Soluções que usem somente método de detecção por assinatura não serão aceitas;

15.4.5. Deverá possuir mecanismo de análise comportamental;

15.4.6. Deverá ser capaz de proteger ataques provenientes de malwares;

15.4.7. Deverá ser capaz de realizar proteção contra ameaças mesmo estando o dispositivo não conectado à internet;

15.4.8. Deverá permitir criar bloqueios personalizados, baseado no nome do aplicativo, caminho do aplicativo e hash do arquivo;

15.4.9. Deverá ser capaz de detectar, alertar e prevenir quando for detectado alguma ameaça;

15.4.10. Deverá ser capaz de prover proteção contra ataques que explorem vulnerabilidades do sistema operacional do host, de acordo com o estabelecido no item 2.18.1 deste Anexo;

15.4.11. Deverá possuir proteção contra BOTs e variantes;

15.4.12. Deverá efetuar proteção permanente e em tempo real dos processos em memória;

15.4.13. Processos suspeitos deverão ser bloqueados;

15.4.14. Deverá possuir mecanismos de análise avançada para proteção e remediação de vírus de código polimorfos, ofuscados, criptografados e contra ameaças avançadas e persistentes, que não são detectadas pelos métodos convencionais de antivírus;

15.4.15. Deverá ser capaz de detectar variações de malwares geradas em memória principal;

15.4.16. Deverá oferecer tecnologia de proteção baseada em técnicas de Inteligência Artificial do tipo Machine Learning;

15.4.17. Em casos de aplicações com comportamento malicioso detectado, deverá efetuar bloqueios de processos e efetuar isolamento de comunicação;

15.4.18. Deverá oferecer proteção contra ataques de 0Day (dia zero);

15.4.19. Deverá oferecer proteção contra Ransomwares, com capacidade de avaliar processos criptográficos em execução no sistema, exclusão de backups, número alto de operações de I/O no sistema de arquivos;

15.4.20. Deverá informar o nome ou endereço IP da origem do ataque ou infecção;

15.4.21. Deverá ter a capacidade de bloquear ataques direcionados a aplicações em execução no servidor através de funcionalidade de proteção contra vulnerabilidades conhecidas e catalogadas através de CVE ou catálogo próprio, tanto para o sistema operacional quanto para aplicações instaladas no servidor;

15.4.21.1. O mecanismo deverá proteger no mínimo os seguintes softwares de terceiros: Apache, Tomcat, JBoss, Microsft IIS, SQL Server, PostgreSQL, Banco de Dados Oracle, MySQL e variantes, Wordpress, Joomla, Adobe entre outros;

15.4.22. Em caso de ataque a solução deverá detectar comportamentos maliciosos da aplicação web;

15.4.23. Para sistemas operacionais windows a solução deverá gerenciar o seu Firewall ou possuir Firewall bidirecional com detecção e proteção contra intrusões e ataques.

15.4.23.1. Firewall deverá possibilitar ações como permitir e bloquear: portas, range de portas, IPs, range de IPs e redes;

15.4.23.2. Deverá ser possível aplicar regras de permitir todo tráfego ou bloquear todo tráfego;

15.4.24. Deverá oferecer funcionalidade de controle de aplicações, identificando aplicações no mínimo pelo código Hash do executável, caminho e nome do aplicativo malicioso;

15.4.25. Deverá oferecer proteção contra vírus de macro e por scripts variados, incluindo bash e powershell;

15.4.26. Deverá oferecer mecanismo de bloqueio baseado em análise realizada pela central de inteligência do fabricante oriundo na nuvem;

15.4.27. Deverá implementar técnicas de Detecção e Resposta (EDR) para prover detecção e investigação para atividades suspeitas

15.4.28. Deverá possibilitar visualizar toda a cadeia de ataque, inclusive os processos e aplicativos executados, arquivos e registros utilizados, endereços acessados, dentre outros;

15.4.29. Deverá oferecer proteção para alterações suspeitas de registro;

15.4.30. Deverá prover mecanismos para criação proteções personalizadas para detecção;

15.4.31. Deverá oferecer proteção contra processos que tentem alterar ou manipular indevidamente os componentes instalados e em execução do antivírus (autoproteção);

15.4.32. Deverá oferecer proteção contra ataques direcionados;

15.4.33. Deverá gerar log local assim como envia-los para a gerência, ou enviar logs em tempo real para a gerência centralizada;

15.4.34. Deverá permitir inclusão de exceções aplicações e caminhos;

15.4.35. A solução deverá oferecer proteção para ameaças em execução:

15.4.35.1. Na memória principal (RAM);

15.4.35.2. Em arquivos;

15.4.35.3. No tráfego de rede;

15.4.35.4. Em dados provenientes de browsers de navegação web (downloads, scripts, etc);

15.4.35.5. Em arquivos compactados (formatos zip, exe, cab, rar, etc);

15.4.35.6. Em processos de inicialização automática;

15.4.35.7. Em serviços criados/modificados;

15.4.36. Solução deverá efetuar a proteção permanente, em tempo real, quando arquivos forem acessados, lidos, gravados, alterados ou renomeados;

15.4.37. Deverá possibilitar a criação de lista de aplicações confiáveis (lista de exceções), a partir da gerencia centralizada, para eliminação de detecções do tipo falso positivo;

15.4.37.1. Deverá oferecer a possibilidade de editar esta lista, com inclusão e remoção de aplicativos;

15.4.38. Deverá possuir a capacidade de detectar antivírus de outros fabricantes que possam acarretar em incompatibilidade;

15.4.39. Deverá impedir execução e instalação de aplicativos cujo comportamento seja suspeito ou que constem na lista de aplicativos inseridos na gerência centralizada;

15.4.40. Deverá detectar e proteger em tempo real o computador contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de páginas da web e scripts em linguagens tais como javascript, vbscript, activex, etc;

15.4.41. Deve oferecer ou executar uma das seguintes opções de ações corretivas para programas maliciosos detectados: bloquear o objeto, executar a limpeza da ameaça e executar ação de quarentena;

15.4.42. Os mecanismos de proteção deverão ser executados sem comprometer o desempenho dos computadores, de forma a não influenciar negativamente no rendimento de aplicações em servidores;

15.4.43. No mínimo as seguintes ocorrências deverão ser registradas em arquivo de log local ou enviadas para a gerência centralizada:

15.4.43.1. Atualização de engine e/ou repositório de vacinas.

15.4.43.2. Recebimento de políticas e tarefas da gerência;

15.4.43.3. Inicialização e finalização de varreduras, agendadas ou manuais, ou quando realizada por meio de análise dos processos em tempo real baseado em machine learning;

15.4.43.4. Detecção de alguma ameaça, registrando no mínimo as seguintes informações:

a) Nome da ameaça;

b) Tipo da ameaça;

c) Arquivo ou local infectado;

d) Data e hora da detecção;

e) Mecanismo que gerou a detecção (varredura agendada, manual, em tempo real);

f) Nome da máquina/endereço IP;

g) Ação realizada;

h) Usuário logado no sistema;

15.4.44. Deverá buscar por itens de atualização nos repositórios, configurado pela gerência, de acordo com topologia e políticas especificadas;

15.4.45. Deverá possibilitar mais de uma versão da ferramenta e seus insumos, para que em casos de incompatibilidades decorrentes de atualizações, seja possível reinstalar versões anteriores estáveis ou instalar versões novas em grupos específicos, para fins de testes de compatibilidade antes de instalação em todo parque;

15.4.46. Deverá fornecer informações do status do agente e de seus componentes, através da gerência com informações atualizadas com delay máximo de 5 minutos;

15.4.47. Deve ser disponibilizado nos idiomas: português (preferencialmente) ou inglês;

AMBIENTE TECNOLÓGICO

15.5. Plataforma de Hardware e software;

15.5.1. Sistemas operacionais utilizados em servidores:

15.5.1.1. Windows Server 2012 (64 bits) e superiores (170 Máquinas).

15.5.1.2. Linux Server (64 bits) (130 Máquinas).

15.5.2. Software utilizados nas estações clientes:

15.5.2.1. Windows 8.1, 10 e 11(500 máquinas);

15.5.2.2. Antivírus McAfee.

15.5.3. Browsers de mercado:

15.5.3.1. Chrome;

15.5.3.2. Internet Explorer;

15.5.3.3. Mozilla Firefox;

15.5.3.4. Microsoft Edge.

15.5.4. Ambiente de virtualização:

15.5.4.1. VMware Vsphere;

15.5.5. Ferramentas de backup:

15.5.5.1. Veeam.

GARANTIA E ATUALIZAÇÃO DAS LICENÇAS

15.5.6. A garantia técnica deverá ser contratada junto ao fabricante da solução, e sua vigência não poderá ser inferior ao período de 36 (trinta e seis) meses, contados a partir da aceitação definitiva da solução;

15.5.7. O atendimento do serviço de suporte técnico da garantia, deverá ser feito por intermédio da CONTRATADA ou diretamente com a fabricante através de portal específico para fins de suporte ou por e-mail;

15.5.8. A garantia técnica deverá ser acionada nas situações específicas onde a CONTRATADA não conseguir solução para o problema ou quando o problema for detectado em relação aos elementos da solução contratada, tais como bugs ou algum mal funcionamento;

15.5.9. A garantia técnica deverá incluir o fornecimento das atualizações do fabricante para a solução;

15.5.10. As atualizações deverão ser fornecidas independente de solicitação da CONTRATANTE.

15.5.11. Deverão ser providas atualizações das listas de definições de vírus e demais insumos para funcionamento atualizado da solução, de acordo com o mercado;

15.5.12. Deverá permitir atualizações da engine do agente (software), assim como da base de dados, padrões de comportamento e quaisquer outros elementos pertinentes à solução;

15.5.13. A garantia técnica contempla suporte técnico do fabricante, serviços de manutenções e atualizações da solução antivírus, base de dados de vacinas, bem como disponibilização de:

15.5.14. Solução de problemas que afetem elementos da solução, incluindo os softwares, atualizações e instalação, evoluções, patches, correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades, novos módulos, adequações e esclarecimento de dúvidas;

15.5.15. Manuais dos produtos e serviços ofertados, base de conhecimento para soluções conhecidas, canal de comunicação, esclarecimento de dúvidas e quaisquer outras informações solicitadas pela CONTRATANTE:

a) As informações prestadas deverão ser disponibilizadas preferencialmente no idioma Português do Brasil ou na falta deste, obrigatoriamente no idioma em Inglês;

15.5.16. Novas versões da solução lançadas pelo fabricante e lançamento de novos softwares em substituição da solução contratada, em caso de descontinuação do software fornecido.

15.5.17. Os serviços descritos neste item deverão ser prestados mediante abertura de chamado pela CONTRATANTE ou pela CONTRATADA, diretamente no portal de comunicação e suporte do fabricante, realizado por meio de e-mail e site de helpdesk;

15.5.18. A garantia deve incluir o funcionamento do serviço de sandbox e de detecção e resposta durante todo o período de vigência da garantia.

SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE FIREWALL e ANTIVIRUS

15.6. **A CONTRATADA deverá prestar serviços de instalação e configuração da Solução de Segurança de Rede Firewall e antivirus especificada neste Termo de Referência, que compreendem, entre outros, os seguintes procedimentos:**

15.6.1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;

15.6.2. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo a Contratante a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

15.6.3. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);

15.6.4. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;

15.6.5. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

15.6.6. Migração das regras de firewall existentes e aplicáveis à solução ofertada;

15.6.7. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

15.6.8. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas;

15.6.9. Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças;

15.6.10. Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances;

15.6.11. Os serviços devem ser realizados considerando todos os tráfegos internos e externos das localidades de presença do órgão no Distrito Federal;

15.6.12. Repasse de informação das configurações realizadas no formato hands-on de no mínimo 4 horas para a equipe responsável pelo projeto por parte da contratante após validação da migração;

15.6.13. O serviço de instalação, configuração e repasse de informação deverão ser realizados de forma presencial, nos locais informados pela CONTRATANTE;

15.6.14. Após a solução ser colocada em produção, deverá ser monitorada on-site nas dependências da SSPDF pelo prazo mínimo de 36 (trinta e seis) horas corridas e posteriormente, 48 (quarenta e oito) horas úteis para troubleshooting de problemas pós migração a serem cumpridas em horário comercial, observando as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação;

15.6.15. A Licitante vencedora será inteiramente responsável pela migração da solução atual para a nova solução, de forma a não comprometer o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação.

15.6.16. Serão contemplados todos os serviços de instalação física de todos os componentes adquiridos, desde a montagem até a energização dos equipamentos.

15.6.17. Deverá ser fornecido documentação de toda a implementação e configuração dos produtos adquiridos.

15.6.18. Após no máximo 5 (cinco) dias úteis da assinatura do contrato, deverá ser realizada uma reunião presencial no Contratante, com a participação de no mínimo 1 (um) preposto da Contratada e os representantes da equipe do Contratante, com o objetivo de elaborar o plano de migração.

15.6.19. A Contratada deverá apresentar, em até 15 (quinze) dias úteis da assinatura do contrato, para aprovação do Contratante, o projeto executivo contendo o plano detalhado de instalação, configuração e migração, especificando os procedimentos e cronograma a serem adotados.

15.6.20. O Contratante fará análise e validação do projeto executivo e do plano de instalação, configuração e migração, em até 5 (cinco) dias, apontado as devidas correções no documento, ficando a Contratada responsável por ajustar o plano em até 7 (sete) dias úteis, conforme as alterações apontadas pela Contratante.

15.6.21. Fica a critério do Contratante, definir o horário de instalação e configuração dos equipamentos, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno.

15.6.22. A Contratada não poderá realizar terceirização dos serviços objeto deste termo de referência, sendo responsável pela execução do serviço objeto desta contratação

15.6.23. Os serviços de instalação e configuração, para cada um dos itens, devem ser executados por técnicos da futura contratada, certificados pelo fabricante dos equipamentos fornecidos, sendo necessária a apresentação de documentação original que comprove a validade desta(s) certificação(ões) enquanto durar o contrato, que pode ser solicitada a qualquer momento;

15.6.24. A futura CONTRATADA deverá apresentar um Projeto Executivo que deve conter, no mínimo, as seguintes informações:

15.6.24.1. Objetivo dos serviços;

15.6.24.2. Plano de gerenciamento de mudanças, detalhando passo a passo o escopo da migração;

15.6.24.3. Cronograma das atividades que serão realizadas, com os prazos estimados e as diretrizes para cada atividade;

15.6.24.4. Projeto lógico de configuração e diagrama de interconexão dos equipamentos;

15.6.24.5. Nome(s) do(s) gerente(s) de projetos responsável(is) e do(s) técnico(s) responsável(is) pela execução dos serviços;

15.6.24.6. Lista de todos os elementos instalados contendo:

a. Nome e endereço IP do equipamento;
b. Equipamento e porta na qual o equipamento foi conectado;
c. Local de instalação (prédio, andar, sala);
d. Número de série do equipamento.

15.6.25. O Projeto Executivo deverá ser entregue pela futura CONTRATADA em até 15 (quinze) dias úteis após a assinatura do contrato, o qual deverá ser aprovado pela CONTRATANTE; os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes.

15.6.26. A instalação e configuração da solução compreenderá dentre outros atendimentos, no mínimo, os seguintes requisitos:

15.6.26.1. Acondicionamento dos equipamentos nos locais de instalação, incluindo a desembalagem, a montagem de todos os componentes que integram a solução, a instalação dos conjuntos montados nos rack padrão 19” da CONTRATANTE, a energização do equipamento, incluindo o fornecimento de eventuais réguas, caso necessário, devendo seguir obrigatoriamente os manuais técnicos do fabricante;

15.6.26.2. Instalação dos transceivers e outros acessórios em seus respectivos slots;

15.6.26.3. Ligações de rede dos equipamentos a infraestrutura da CONTRATANTE, incluindo o fornecimento, quando necessário, de:

1. Cordões ópticos OM4 com, no mínimo, 2 (dois) metros de comprimento para ligações em fibra;
2. Patch-cords UTP CAT6A com, no mínimo, 2 (dois) metros de comprimento para ligações em par metálico;
3. Os cabos/cordões necessários para a interligação de servidores, usuários e outras conexões que não as estritamente fornecidas são de responsabilidade da CONTRATANTE, ou seja, cabe a CONTRATADA interligar os equipamentos fornecidos.
4. Upgrade ou Downgrade do firmware;
5. A realização dos ajustes de hardware e software necessários ao funcionamento do ambiente e a instalação da solução de gerenciamento;
6. Conexão das interfaces de gerenciamento a nova rede out-of-band e testes de acesso a ferramenta de gerência para administração;
7. Configuração e teste de envio de Traps SNMP; Verificações dos recursos e o seu perfeito funcionamento e integração com os demais, conforme as melhores práticas indicadas pelo fabricante;
8. A identificação dos equipamentos e de todas as suas conexões.

15.6.27. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, podendo estas ser realizadas presencialmente, por telefone ou via conferência web, devendo a futura CONTRATADA sugerir as configurações de acordo com normas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

15.6.28. A Contratada deverá configurar todas as funcionalidades do produto licenciadas e solicitadas pela Contratante;

15.6.29. As configurações deverão seguir fielmente a padronização previamente estabelecida pela CONTRATANTE;

15.6.30. Durante o processo de instalação e configuração deverá ser realizada transferência de conhecimento para a equipe da Contratante;

15.6.31. A futura CONTRATADA deverá fazer análise do ambiente tecnológico atual, devendo a CONTRATANTE fornecer todas as informações necessárias sobre a infraestrutura instalada, de modo que se possa garantir a continuidade dos serviços prestados pelo órgão durante a migração, mantendo a disponibilidade dos serviços básicos de rede (resolução de nomes, endereçamento dinâmico, autenticação dos usuários, etc.) e dos demais serviços de retaguarda (aplicativos, correio eletrônico, banco de dados, Internet, etc.);

15.6.32. A substituição da infraestrutura atual deve ser planejada e executada de modo que não cause interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional da CONTRATANTE; caso não seja possível manter a disponibilidade dos serviços básicos no momento da instalação, as manobras de implantação deverão ser realizadas durante janela de manutenção agendada previamente, em horários que não comprometam o funcionamento das atividades do órgão, inclusive aos sábados, domingos e feriados;

15.6.33. Ao término do serviço deve ser fornecido um relatório detalhado (as-built) contendo todas as configurações realizadas, com comentários sobre os principais comandos e as justificativas das opções de parametrização de modo a facilitar a posterior administração da solução e a continuidade de seu funcionamento;

15.6.34. O relatório deve conter, no mínimo, as seguintes informações:

15.6.34.1. Diagrama de arquitetura da solução;

15.6.34.2. Procedimento operacional detalhado com as etapas de instalação e configuração;

15.6.34.3. Informações de monitoramento da solução;

15.6.34.4. Informações pertinentes a posterior continuidade e manutenção da solução;

15.6.34.5. Referências da documentação oficial do produto.

15.6.35. A critério da CONTRATANTE, poderá ser elaborado um único as-built contendo todas as informações de todos os equipamentos e softwares instalados/configurados;

15.6.36. O serviço de instalação e configuração somente será concluído após a apresentação pela contatada do projeto executivo, as-built e o recebimento definitivo do serviço pela contratante.

15.6.37. Após a solução ser colocada em produção, deverá ser monitorada on-site nas dependências do Secretaria de Segurança Pública do Distrito Federal pelo prazo mínimo de 36 (trinta e seis) horas corridas e posteriormente, 48 (quarenta e oito) horas úteis para troubleshooting de problemas pós migração a serem cumpridas em horário comercial, observando as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação.

DOS REQUISITOS TECNOLÓGICOS DE PROJETO E DE IMPLEMENTAÇÃO, IMPLANTAÇÃO E METODOLOGIA DE TRABALHO.

15.6.38. A Licitante vencedora será inteiramente responsável pela instalação/configuração e atualização da solução, de forma a não comprometer o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação;

15.6.39. A Licitante vencedora juntamente com a CONTRATANTE deverá realizar o "de/para" da configuração atual dos equipamentos em uso pela SSP/DF, bem como realizar os ajustes que se fizerem necessários mediante solicitação da CONTRATANTE.

15.6.40. Serão contemplados todos os serviços de instalação física e configuração de todos os componentes adquiridos, desde a montagem dos equipamentos até a energização destes;

15.6.41. Deverá ser fornecido documentação de toda a implementação e configuração dos produtos;

15.6.42. Para a instalação e configuração, a CONTRATADA deverá apresentar um Projeto Executivo que deve conter, no mínimo, as seguintes informações:

a) Objetivo dos serviços;

b) Plano de gerenciamento de mudanças, detalhando passo-a-passo o escopo da migração;

c) Cronograma das atividades que serão realizadas, com os prazos estimados e as diretrizes para cada atividade;

d) Projeto lógico de configuração e diagrama de interconexão dos equipamentos;

e) Nome(s) do(s) gerente(s) de projetos responsável(is) e do(s) técnico(s) responsável(is) pela execução dos serviços;

15.6.43. Fica a critério do Contratante juntamente com a Contratada, definir o horário de instalação e configuração dos equipamentos, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno;

15.6.44. A Contratada deverá comunicar à Contratante a conclusão da instalação e configuração dos equipamentos e entregar toda documentação técnica "As Built", que por sua vez deve contemplar todas as informações, juntamente com os ajustes, que se mostraram necessários quando da instalação de fato.

15.6.45. Após a realização do serviço de implantação das soluções contratadas , deverá ser entregue pela CONTRATADA o Relatório Técnico detalhando todos os procedimentos adotados, cujos serviços serão avaliados por um técnico da SSP/SMT.

15.7. Para fins de avaliação do serviço a CONTRATANTE avaliará se o "Relatório de Atividade" está de acordo com procedimentos previstos na Ordem de Serviço, estando de acordo, a CONTRATANTE emitirá Termo de Aceite Definitivo -TAD.

15.7.1. Caberá a CONTRATADA disponibilizar profissionais técnicos devidamente capacitados para a resolução de chamados e esclarecimentos de dúvidas, durante todo o período de suporte técnico e garantia dos produtos.

15.7.2. Profissionais certificados e com experiência comprovada na solução de pelo menos 12 meses.

15.7.3. Todos os atendimentos técnicos deverão ser registrados, cabendo a CONTRATADA apresentar ao CONTRATANTE, sempre que solicitado, Relatório Técnico de Suporte, nele constando a descrição clara do(s) problema(s) identificado(s) e os procedimentos adotados e/ou recomendados para a sua resolução.

15.7.4. Após finalizado o serviço, e entregue o Relatório Técnico, o mesmo será analisado e validado por um representante da Contratante, que emitirá o Termo de Aceite Definitivo-TAD, para fins de pagamento.

REQUISITOS DE CAPACITAÇÃO

15.8. A transferência de conhecimento deve garantir que toda a informação gerada durante os processos de instalação e migração seja integramente apresentada pela equipe da contratada, por meio de métodos expositivos, realização prática das atividades, apresentação de resumos, esquemas, relatórios ou qualquer outro documento que viabilize ou facilite a absorção da tecnologia do novo ambiente pela equipe da contratante.

16. CRONOGRAMA

REQUISITOS TEMPORAIS

16.1. A seguir são listados os requisitos temporais relativos ao objeto:

16.1.1. Assinatura do Contrato (CONTRATANTE e CONTRATADA): Início dos prazos= D

16.1.2. Convocar reunião de Kick-off do Projeto (CONTRATANTE Elaborar e enviar o Termo de Compromisso e Ciência para a CONTRATADA (CONTRATANTE)= D+2

16.1.3. Realização da reunião de Kick-off (CONTRATANTE E CONTRATADA)= D+5

- Apresentação formal do Gestor do Contrato e do Preposto (CONTRATANTE e CONTRATADA);
- Repasse à CONTRATADA de conhecimentos necessários à execução dos serviços (CONTRATANTE);
- Entrega e assinatura dos documentos necessários para gestão e fiscalização (CONTRATANTE);
- Entrega do Termo de Compromisso e Ciência devidamente assinados (CONTRATADA).

16.1.4. Entrega do Projeto de Implantação (CONTRATADA)= D+15

16.1.5. Aprovação do Projeto de Implantação (CONTRATANTE)= D+20

16.1.6. Entrega dos bens (CONTRATADA)= D+60

16.1.7. Início da execução dos serviços e instalação dos bens (CONTRATADA)= D+70

Assinatura de contrato	**Dia 0**						
Reunião Kick-off		**até 5 dias corridos**					
Entrega do Projeto de Implantação			**até 15 dias corridos**				
Entrega do equipamento (Instalação e configuração)				**até 60 dias corridos**			
Início da execução dos serviços e instalação dos bens					**até 70 dias corridos**		
Recebimento provisório						**até 7 dias corridos**	
Recebimento definitivo							**até 15 dias corridos**

16.2. A CONTRATADA deverá entregar os bens em até 60 dias úteis contados da data de assinatura contratual. Esse prazo poderá ser prorrogado por até mais 40 dias, mediante solicitação e justificativa formal da contratada e anuência da contratante;

16.3. Os serviços programados deverão ser prestados, em regra, nos dias úteis, durante o horário de funcionamento do órgão, observados os atendimentos em cenários críticos e de urgência, mediante a abertura de chamado técnico para o caso do suporte técnico, conforme especificado neste Termo de Referência;

16.4. A entrega dos bens deverá estar em conformidade com as políticas do órgão para recebimento de bens e patrimônio;

16.5. O cronograma de todas as atividades programadas, relativas à execução do contrato, deverá ser aprovado pela CONTRATANTE, devendo atender, no mínimo, aos itens e periodicidades deste Termo de Referência;

16.6. Os bens serão recebidos provisoriamente no prazo de 7 dias, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta;

16.7. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades;

16.8. Os bens deverão ser instalados em até 10 dias após o recebimento dos respectivos equipamentos. Este prazo poderá ser prorrogado em mais 10 dias, desde que haja justificativa plausível e que essa seja acatada pela equipe de fiscalização e gestão do contrato que for gerado a partir deste processo;

16.9. Os bens serão recebidos definitivamente no prazo de 15 dias, contados do recebimento provisório, ateste dos respectivos serviços de instalação e configuração, após a verificação da qualidade e quantidade dos equipamentos/material e serviços e consequente aceitação mediante termo circunstanciado de recebimento definitivo;

16.10. Na hipótese da verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo;

16.11. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

17. DOS LOCAIS DE PRESTAÇÃO DO SERVIÇO

17.1. O serviço de será executado presencialmente, nas unidades a a seguir: CIOB **-** Centro Integrado de Operações de Brasília - SAM - Conjunto A bloco "D" - Edifício anexo da Sede da SSP/DF - CEP 70610-640 - Brasília DF, SUDEC - Defesa Civil - SIA Trecho 06, lote 25-35 Ed. Business Center - CEP 71205-060 - Brasília DF, GETRAM - Gerência de Transporte e Manutenção - SIA Trecho 4 Lote 1480 Edifício SENAP I - CEP 71200-040 - Brasília DF. NUAL **-** Núcleo de Almoxarifado e NUPAT - Núcleo de Patrimônio - SGO Quadra 5 Lote 795 CEP 70610-650 - Brasília DF.

18. SUPORTE TÉCNICO AVANÇADO PARA MANUTENÇÃO PREVENTIVA E CORRETIVA DA SOLUÇÃO - PARA OS GRUPOS 1 E 2

18.1. **REQUISITOS DE ATENDIMENTO: GERAIS**

18.1.1. Para melhor entendimento da escala de criticidade do ambiente, a SSP-DF decidiu categorizar os atendimentos em 3 níveis de Severidade a saber:

18.1.2. Severidade 1 (Alta) com prazo máximo para atendimento em até 1 (uma) Hora;

18.1.3. Severidade 2 (Media) com prazo máximo para atendimento em até 3 (três) Horas;

18.1.4. Severidade 3 (Baixa) com prazo máximo para atendimento em até 12 (doze) Horas;

18.1.5. O atendimento pelo fabricante deve estar disponível para todos os componentes da solução ofertada;

18.1.6. O fabricante emitirá relatório sobre todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, em papel ou em arquivo eletrônico, preferencialmente em arquivo texto/planilhas, com informações analíticas e sintéticas dos chamados de garantia/suporte abertos e fechados no período (mensal) , incluindo:

a) Quantidade de ocorrências (chamados) registradas no período;

b) Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura;

c) Data e hora de abertura;

d) Data e hora de início e conclusão do atendimento;

e) Identificação do técnico do CONTRATANTE que registrou o chamado;

f) Identificação do técnico do CONTRATANTE que atendeu ao chamado da garantia;

g) Descrição do problema;

h) Descrição da solução;

i) Informações sobre eventuais escaladas de níveis de suporte;

j) Resumo com a lista de chamados concluídos fora do prazo de solução previamente estabelecido;

k) Total de chamados no mês e o total acumulado até a apresentação do relatório.

18.1.7. O relatório deve ser assinado por representante da CONTRATADA, responsável pelo acompanhamento do serviço, e entregue a SSP-DF, que se obriga a acompanhar a execução das manutenções;

18.1.8. A cada chamado de suporte categorizado como grau de Severidade 1**,** o fabricante deverá disponibilizar um Engenheiro de Suporte na forma de recurso humano, que ao ser notificado, atuará como ponto de apoio e contato, auxiliando na condução do processo internamente junto ao fabricante para fornecer assistência avançada seja por telefone fixo, telefone móvel ou e-mail ou qualquer solução aceita pela CONTRATANTE. Caso este recurso humano esteja temporariamente indisponível, deve ser dada a opção de se escalar o chamado para um Engenheiro de Solução de nível avançado e este devera dar prosseguimento no atendimento até o encerramento do chamado.

18.1.9. O recurso humano designado pelo fabricante deverá manter o cliente informado sobre melhores práticas e *Roadmap* das soluções ofertadas;

a) O contato deste recurso humano designado deverá ser mensal;

b) Entregar relatórios mensais com status e descritivo detalhado das atividades realizadas no cliente, evidenciando a efetividade dos serviços prestados pelo fornecedor;

c) Estes serviços deverão ser prestados exclusivamente na modalidade remota, utilizando-se de ferramentas de acesso remoto através da Internet e permitida pelo Órgão (tal como Webex), com total segurança e criptografia de dados, de forma que os recursos técnicos consigam acessar remotamente os servidores ;

d) Prestar assessoria proativa e reativa nas questões relativas às atualizações, patches e alertas de impacto.

e) Apresentar um relatório trimestral demonstrando a saúde do ambiente dos produtos escopo deste fornecimento;

f) Propor melhorias no ambiente;

g) Será efetuada Manutenção corretiva, sempre que a solução apresentar falhas que impeçam o seu funcionamento normal e/ou requeiram a intervenção de técnico especializado;

h) As manutenções preventivas e corretivas serão de responsabilidade do CONTRATADO, sem custos adicionais ao CONTRATANTE;

i) Atuar junto ao Suporte do fabricante na escalada de problemas críticos e com acompanhamento do problema até a resolução;

18.1.10. Possuir atendimento com consultores na língua portuguesa;

18.1.11. Monitorar e gerenciar questões de escalada e servir como ponto único de contato técnico.

18.1.12. Fornecer subsídios a CONTRATANTE relativo a incidentes para identificação de diagnóstico.

18.1.13. Auxiliar na solução de problemas fornecendo detalhes técnicos para a análise de causa provável de problemas encontrados.

18.1.14. Todos os prazos para atendimento, em se tratando da Garantia, começarão a ser contados a partir da abertura do chamado independentemente deste ter sido feito via telefone, e-mail, Website do fabricante;

18.1.15. *A CONTRATADA deve fornecer Nome, CPF e função do técnico que virá a SSP, atender a demanda;*

a) ***O técnico devera comparecer ao ambiente devidamente identificado, portando sempre um crachá da empresa. Sem este documento (crachá), não será permitida a sua entrada no ambiente;***

18.1.16. **REQUISITOS DE ATENDIMENTO: NÍVEL MÍNIMO DE SERVIÇO E CRITICIDADE - SUPORTE**

18.1.17. Por início de atendimento entende-se a alocação de técnico devidamente qualificado para efetuar a correção do problema ou o *troubleshooting* preciso, com interlocução direta com a equipe da SSP-DF.

18.1.18. A abertura da chamada deverá ser realizada pela CONTRATANTE em sistema web/app ou telefone, com acesso garantido pela CONTRATADA e linguagem em português, o que implicará na imediata abertura de uma Ordem de Serviço (O.S);

18.1.19. O suporte técnico deverá ser prestado para cada solução adquirida e deverá ser acionado em caso de qualquer indisponibilidade da solução, devendo haver o atendimento "on-site", no endereço constante deste Termo, se requerido pelo CONTRATANTE, conforme os índices de criticidade abaixo:

18.1.20. **CRITICIDADE**

Severidade	Descrição	Prazo Máximo de Atendimento
Severidade 1 (Alta)	**Equipamento ou Sistema Inoperante:** Entende-se como sistema ou equipamento inoperante, aqueles que não estejam funcionando em sua capacidade total de recursos com impacto direto nas operações críticas de negócio. *Exemplos*: Servidor de produção ou outro Sistema inicial está inativo. **Equipamento ou Sistema Parado:** Entende-se como sistema ou equipamento parado, aqueles que se encontram sem nenhum tipo de funcionamento. *Exemplos:* Servidor de produção ou outro Sistema não emite sequer sinal de ligado ou desligado; · Parte substancial dos dados essenciais corre risco de perda ou corrupção; · Operações relacionadas ao negócio foram afetadas, foi detectada falha que compromete a integridade geral do Sistema ou dos seus dados. **Alto impacto no ambiente de produção ou grande restrição de funcionalidade:** *Exemplos*: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade em longo prazo possa ser afetada negativamente.	Com a O.S. aberta a CONTRATADA, registrará as informações: quem abriu, quem recebeu pela empresa, data e hora do início da atividade; Abre-se um prazo inicial de 15 (quinze) minutos a partir do horário da abertura do chamado para a devida resolução do problema de modo ***REMOTO*** ; Findado este prazo inicial de até 15 (quinze) minutos para a resolução do problema de modo ***REMOTO*** e constatada a inoperância ou permanência do problema, a empresa CONTRATADA será novamente notificada da concessão de um novo prazo de mais 15 (quinze) minutos, para a urgente ALOCAÇÃO de um técnico visando o atendimento ***IN LOCO*** nos endereços físicos pré determinados por esta Secretaria, (mantido o número da O.S. inicialmente aberta com as respectivas informações); - A partir da ALOCAÇÂO deste técnico, conforme o Nível de Severidade 1 estabelece, a empresa terá mais 30 (trinta) minutos para a resolução do problema; **PRAZO MÁXIMO TOTAL PARA ATENDIMENTO**: **Até 1 (uma) Hora**; ** Representante técnico especialista do suporte deve estar disponível 24 x 7 e ser automaticamente notificado na abertura da O.S.*
Severidade 2 (Média)	**O defeito não gera impacto ao negócio.** *Exemplo:* Ocorreu um erro que causou impacto negativo limitado nas operações. Funcionalidades principais prejudicadas. Operação prossegue com restrições significativas. Perda de funcionalidades não críticas.	Com a O.S. aberta a CONTRATADA, registrará as informações: quem abriu, quem recebeu pela empresa, data e hora do início da atividade; Abre-se um prazo inicial de até 1 (uma) hora onde um Engenheiro de Suporte do fabricante deve iniciar o atendimento de modo ***REMOTO*** ou por telefone. Findado este prazo inicial de até 1 (uma) hora para a resolução do problema de modo ***REMOTO*** e constatada a inoperância ou permanência do problema; a empresa CONTRATADA será novamente notificada da concessão de um novo prazo de 2 (duas) horas, para o DESLOCAMENTO de um técnico (mantido o número da O.S. inicialmente aberta com as respectivas informações) visando o atendimento ***IN LOCO*** nos endereços físicos predeterminados por esta Secretaria.; **PRAZO MÁXIMO TOTAL PARA ATENDIMENTO**: Até 3 (três) Horas; ** Representante técnico especialista do suporte deve estar disponível 24 x 7 e ser automaticamente notificado na abertura da O.S.*
Severidade 3 (Baixa)	**O problema é pequeno, ou de documentação.** *Exemplos:* O problema não afetou as operações da contratante negativamente; mas o usuário continua a utilizar a solução; encaminhamento de solicitações, sugestões para novos recursos ou aprimoramento do software licenciado; esclarecimento de dúvidas (dos produtos deste fornecimento) ou em períodos de mudanças complexas no ambiente que ensejem a incorporação temporária de expertise, para realizar tarefas pré-determinadas	Com a O.S. aberta a CONTRATADA, registrará as informações: quem abriu, quem recebeu pela empresa, data e hora do início da atividade; Abre-se um prazo inicial de até 3 (tês) horas onde um Representante Técnico do Suporte do fabricante deve iniciar o atendimento de modo ***REMOTO*** ou por telefone. Findado este prazo inicial de 3 (três) horas para a resolução do problema de modo ***REMOTO*** e constatada a inoperância ou inconsistência da resolução do problema; a empresa CONTRATADA será novamente notificada da concessão de um novo prazo de mais 9 (nove) horas, para o DESLOCAMENTO, caso seja necessário e a critério da CONTRATANTE, de um técnico (mantido o número da O.S. inicialmente aberta com as respectivas informações) aos endereços físicos predeterminados por esta Secretaria. **PRAZO MÁXIMO TOTAL PARA ATENDIMENTO**: Até 12 (doze) Horas;

Severidade	Descrição	Prazo Máximo de Atendimento
		** Representante técnico especialista do suporte deve estar disponível 8 x 5 e ser automaticamente notificado na abertura da O.S.*

18.1.21. **É vedado o cancelamento, encerramento dos chamados ou recategorização** dos níveis de Severidade pela CONTRATADA sem a autorização prévia e expressa da CONTRATANTE;

18.1.22. Todos os profissionais que irão trabalhar de alguma maneira no contrato, inclusive técnicos e gerentes da empresa CONTRATADA, devem ser previamente cadastrados (e assinar Termo de Confidencialidade e Sigilo), para acesso remoto, inclusive.

18.1.23. O período de suporte deve estar diretamente atrelado ao período de garantia da solução;

18.1.24. Não será cobrado serviço mensal para os serviços de suporte, uma vez que os reparos dos equipamentos serão realizados durante a vigência de garantia ;

18.1.25. Dentro do prazo máximo de solução do chamado está compreendido o prazo de atendimento;

18.1.26. Dentro do prazo máximo de atendimento do chamado, cabe ao fornecedor dar início, junto ao CONTRATANTE, às providências que serão adotadas para a solução deste chamado;

18.1.27. Considera-se plenamente solucionado o problema quando forem restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa ou de contorno;

18.1.28. Não se encaixam nos prazos descritos nos itens referentes aos problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução;

18.1.29. Para esses problemas, o fornecedor deverá, de acordo com os prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução paliativa que deve ser expressamente autorizada pela CONTRATANTE;

18.1.30. Nos casos em que as manutenções necessitarem de paradas momentâneas da solução, a CONTRATANTE deverá ser imediatamente notificada para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

18.1.31. Durante o período de vigência do contrato, o fornecedor executará, sem ônus adicionais, todas as correções de falhas (bugs) do equipamento;

18.1.32. Durante o período de vigência do contrato A CONTRATADA deverá garantir que todas as atualizações do equipamento fornecidas devem ser da última e mais atual versão disponível, quando da data da entrega dos equipamentos, e que serão totalmente aplicáveis sem necessidade de alterações ou adaptações estruturais que demandem custos adicionais à CONTRATANTE.

18.1.33. A CONTRATADA deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento de novas versões por necessidade de correção de problemas ou por implementação de novos releases, a partir da assinatura do Termo de Aceite, durante todo o período de garantia.

18.1.34. Para fins de comprovação de assistência técnica autorizada deverá ser encaminhado, quando da assinatura do contrato, documento probatório dessa condição, sendo o mesmo passível de confirmação junto ao fabricante.

18.2. **REQUISITOS DE ATENDIMENTO: CANAIS**

18.2.1. O suporte técnico deve estar disponível para abertura de chamados técnicos 24 horas por dia, 7 dias por semana, mediante sistema "website" do fabricante (*Web/app)* e telefone (0800 ou número local em Brasília);

18.2.2. Considera-se como dia útil para a SSP-DF o período que se inicia as 7:00 (sete) horas da manhã e finda as 19:00 (dezenove) horas da noite;

18.2.3. Em caso de indisponibilidade do canal de atendimento, os chamados técnicos poderão ser abertos via e-mail, "website" do fabricante e telefone;

18.2.4. O fornecedor precisa possuir e informar seu endereço com página ativa na Internet do fabricante, onde deverão estar disponíveis e acessíveis todos os drivers atualizados, últimas versões do firmware e demais informações sobre detalhes técnicos dos equipamentos.

18.3. **DA HOMOLOGAÇÃO, GARANTIA DOS PRODUTOS, MANUTENÇÃO E NÍVEIS DE SERVIÇOS**

18.3.1. A titulo de agilizar a análise por parte da equipe técnica desta Secretaria, será exigida dos licitantes a comprovação de que os itens cotados na Proposta Comercial devem ter a sua equivalência (com descritivos técnicos e datasheets) comprovada na Proposta Técnica do licitante, com a respectiva identificação do nome do arquivo e numero da página onde se encontram as informações solicitadas pelo CONTRATANTE;

18.3.2. A NÃO observância a este preceito, implicará na imediata desclassificação do licitante;

18.3.3. A empresa vencedora será responsável pela entrega dos equipamentos na sede da SSP/DF, sem nenhum tipo de ônus para a CONTRATANTE, no prazo de até 30 (trinta) dias corridos a partir da assinatura do contrato ou emissão da nota de fornecimento ou emissão do empenho.

18.3.4. O prazo de garantia começará a transcorrer com a emissão do **Termo de Recebimento Definitivo**;

18.3.5. O prazo de garantia estabelece-se em função do valor a ser gasto na aquisição e do tempo de vida útil do equipamento. Com um prazo maior de garantia, não será necessário realizar possíveis gastos com aquisição de peças de reposição durante sua vida útil;

18.3.6. Durante o prazo de garantia será substituída sem ônus para a CONTRATANTE, a parte ou peça defeituosa:

18.3.7. Os serviços de reparo físico dos equipamentos serão executados somente e exclusivamente IN LOCO;

18.3.8. Todas as peças possivelmente substituídas deverão ser homologadas pelo fabricante do equipamento;

18.3.9. A peça ou equipamento defeituoso deverá ser substituído(a) por equipamento novo, de primeiro uso e de modelo igual ou superior ao danificado, ao qual passará à propriedade da CONTRATANTE, sendo imediatamente incluído(a) no Contrato de manutenção vigente em substituição ao equipamento danificado/substituído;

18.3.10. Todas as atividades que exijam a paralisação ou causem comprometimento de serviços de informática em produção deverão ser executados nos horários acordados com a CONTRATANTE.

18.3.11. O equipamento que for identificado como defeituoso, deverá ser reparado no prazo máximo de 2 (dois) dias úteis, a contar do atendimento ao chamado de garantia, resguardados os prazos contidos na Tabela de Criticidade, citada anteriormente;

18.3.12. A Contratada deverá prestar assistência técnica aos equipamentos e acessórios (softwares, cabos, baterias, carregadores, etc.), contra defeitos de fabricação, durante o período de garantia, na forma e prazos a seguir especificados, a fim de mantê-los em perfeito funcionamento, sob as condições normais de utilização, através de rede mantida pelo fabricante ou por ele credenciada, apresentando, para tanto, o Termo de Garantia e Suporte Técnico;

18.3.13. A CONTRATADA deverá possuir assistência técnica autorizada pelo fabricante do equipamento, comprovação esta ratificada em carta de autorização endereçada pelo fabricante à CONTRATADA;

18.3.14. A assistência técnica será prestada na modalidade on-site, durante o período de garantia de 36 (trinta e seis) meses para os equipamentos que compõem esta **Solução de Segurança Computacional,** canal de atendimento e chamado técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de site na Internet e/ou canal telefônico gratuito 0800 e consistirá na reparação dos equipamentos, com a substituição de peças e componentes que se fizer necessária, de acordo com os manuais e as normas técnicas pertinentes;

18.3.15. Eventual pedido de prorrogação do prazo de reparo somente será deferido se apresentado tempestivamente, por escrito, devidamente justificado, e o equipamento defeituoso for substituído por outro equivalente ou de configuração superior em perfeitas condições de uso, que ficará à disposição do Contratante até o retorno do equipamento reparado;

18.3.16. A assistência técnica utilizará apenas peças e componentes novos e originais;

18.3.17. O fornecedor concederá à CONTRATANTE garantia integral durante o período de vigência do contrato, com atendimento 24 horas por dia e 7 (sete) dias por semana, a contar da data de homologação do produto, contra qualquer defeito ou problema em toda a solução, incluindo avarias no transporte dos equipamentos até o local de entrega, mesmo ocorrida sua aceitação/aprovação pelo contratante;

18.3.18. O fornecedor garante, durante o período de vigência do contrato o fornecimento dos componentes referentes ao hardware e software, para fins de manutenções e suporte técnico; de forma que possam ser mantidas todas as funcionalidades dos equipamentos e soluções inicialmente contratadas. Caso ocorra neste período a descontinuidade de fabricação de componentes, deverá ser também garantida à total compatibilidade dos itens substitutos com os itens originalmente fornecidos;

18.3.19. Durante o período de vigência do contrato e da comprovação de sua respectiva Garantia, qualquer componente que apresente defeito ou mau funcionamento, sem indicação de solução, deverá ser substituído em um prazo máximo de até 2 (dois) dias úteis.

18.4. **DOS REQUISITOS TECNOLÓGICOS DE EXPERIÊNCIA PROFISSIONAL**

18.4.1. A LICITANTE deverá apresentar Atestados de Capacidade Técnica (ACT) emitidos por órgão público comprovando que executou serviços de fornecimento, instalação, configuração e suporte de Firewall NGFW com as características descrita nesse estudo;

18.4.2. A LICITANTE deverá apresentar Atestados de Capacidade Técnica (ACT) emitidos por órgão público comprovando que executou serviços de fornecimento, instalação, configuração e suporte de soluções de EDR com as características descrita nesse estudo;

18.5. **DOS REQUISITOS TECNOLÓGICOS DE FORMAÇÃO DA EQUIPE QUE EXECUTARÁ**

18.5.1. A CONTRATADA deverá apresentar pelo menos 2 (dois) profissionais certificados pelo fabricante nas soluções descritas nesse estudo a fim de realizar o projeto, implantação e configuração da solução;

19. **DA QUALIFICAÇÃO TÉCNICA**

19.1. As empresas licitantes deverão apresentar comprovação de aptidão no desempenho de atividade pertinente, para os GRUPOS 1 e 2, compatível em características com os objetos desta licitação, por intermédio da apresentação de Atestado(s) de Capacidade Técnica, fornecido(s) por pessoa jurídica de direito público ou privado.

19.1.1. Considera(m)-se compatível(eis) o(s) atestado(s) que expressamente certifique(m) que o proponente já prestou serviços pelo menos 50% (cinquenta por cento) do quantitativo a ser contratado, estabelecido neste Termo de Referência, de acordo com o TCU, Acórdãos de Plenário nº 1.284/2003, nº 2.068/2004, nº 2.088/2004, nº 2.656/2007, nº 2.056/2008 e nº 11.213/2013.

19.1.2. Será permitido a soma de atestado(s), visando comprovar o quantitativo de 50% (cinquenta por cento) estabelecido acima.

19.2. O atestado deverá ser em língua portuguesa do Brasil, onde deverá indicar dados da entidade emissora e dos signatários do documento, além da descrição do objeto, quantidades e prazos da prestação dos serviços.

19.3. As empresas licitantes poderão realizar visita às instalações dos locais de prestação do serviço, a qual deverá ser agendada até 01 (um) dia útil antes da data fixada para a abertura da sessão pública, com o objetivo de inteirar-se das condições e grau de dificuldades existentes, perante à Subsecretária de Modernização e Tecnologia da SSPDF, por meio dos telefones (61) 3441-8820 ou (61) 3441-8771 e-mail cinf@ssp.df.gov.br.

19.4. As empresas licitantes que optarem por realizar a visita deverão apresentar junto com a documentação de habilitação o Atestado de Visita técnica, conforme modelo que segue como Anexo V de Termo de Referência, que será emitido pela SMT/SSPDF, em nome da empresa licitante, de que esta, por intermédio de seu representante, vistoriou as instalações onde serão executados os serviços objeto deste Termo de Referência, tomando conhecimento de todos os aspectos que possam influir direta e indiretamente na execução do mesmo.

19.5. As empresas licitantes que não optarem por realizar a visita deverão apresentar junto com a documentação de habilitação declaração de desistência de visita técnica, conforme modelo que segue como Anexo VI, devidamente assinado pelo responsável da proponente.

19.6. Os custos pertinentes à vistoria aos locais dos serviços correrão por exclusiva conta da licitante, não cabendo à SSPDF qualquer tipo de indenização.

19.7. Em nenhuma hipótese a licitante poderá alegar desconhecimento dos locais e de suas condições para elaboração da sua proposta, bem como para a execução do contrato e cumprimento das obrigações decorrentes.

19.8. **Declaração da licitante informando que cumpre o disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991, com reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação:**

> Art. 93. A empresa com 100 (cem) ou mais empregados está obrigada a preencher de 2% (dois por cento) a 5% (cinco por cento) dos seus cargos com beneficiários reabilitados ou pessoas portadoras de deficiência, habilitadas, na seguinte proporção:
>
> I - até 200 empregados.....2%;
>
> II - de 201 a 500.....3%;

III - de 501 a 1.000.....4%;

IV - de 1.001 em diante. .....5%.

20. DA GARANTIA CONTRATUAL

20.1. Será exigida da CONTRATADA a apresentação, **no prazo máximo de 10 (dez) dias úteis da assinatura do termo contratual**, de garantia em favor da CONTRATANTE, correspondente a **2% (dois por cento) do valor total do contrato**, numa das seguintes modalidades, conforme opção da CONTRATADA:

20.1.1. caução em dinheiro ou títulos da dívida pública federal.

20.1.2. seguro-garantia.

20.1.3. fiança bancária.

20.1.4. O prazo para entrega da garantia poderá ser prorrogado uma única vez, por igual período, caso necessário, desde que a justificativa fundamentada seja previamente apresentada para análise da CONTRATANTE antes de expirado o prazo inicial.

20.1.5. A garantia contratual na porcentagem de 2**%** (dois por cento) do valor do contrato, foi estabelecida, visando minimizar os riscos da inexecução contratual, sendo ato discricionário da Administração, imposto para garantir o sucesso total da contratação, conforme parágrafo único do Art. 98, da Lei nº 14.133/22.

21. DO ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO

21.1. Serão nomeados Gestor e/ou Fiscal do contrato para acompanhar e fiscalizar a execução dos contratos, conforme o disposto nas normas que regem o tema de Tecnologia da Informação no Distrito Federal, consideradas as peculiaridades do caso.

21.2. A gestão, fiscalização e o controle da execução do contrato, bem como da prestação dos serviços de instalação, garantia, assistência técnica, atualização e suporte será exercida por servidor (es) designado (s) para desempenhar esta função, com poderes para praticar quaisquer atos que se destinem a preservar os direitos da CONTRATANTE, devendo o mesmo franquear à CONTRATADA livre acesso aos locais de execução dos trabalhos, bem como aos registros e informações sobre o contrato;,

21.3. Esse (s) servidor (es) anotará em registro próprio todas as ocorrências, determinando o que for necessário à regularização das faltas ou defeitos observados;

21.4. A fiscalização de que trata este tópico não exclui, nem reduz, a responsabilidade da CONTRATADA, inclusive resultante de imperfeições técnicas, vícios ou emprego de material inadequado ou de qualidade inferior, e na ocorrência desses, não implica corresponsabilidade da CONTRATANTE ou de seus agentes;

21.5. O (s) executor (es), durante seu mister, deve (m) agir de forma proativa e preventiva, observar o cumprimento pela CONTRATADA das regras previstas no instrumento contratual, buscar os resultados esperados no ajuste e trazer benefícios e economia para esta Secretaria, devendo cumprir integralmente a Portaria nº 119-SSPDF, que estabelece diretrizes para a gestão, acompanhamento e fiscalização da execução de contratos, convênios, acordos e instrumentos congêneres celebrados pela SSPDF;

21.6. Sem prejuízo de outras atribuições legais, poderá a fiscalização da CONTRATANTE:

21.7. Determinar as medidas necessárias e imprescindíveis à correta execução do objeto, bem como fixar prazo para as correções das falhas ou irregularidades constatadas;

21.8. Sustar quaisquer fornecimentos/serviços que estejam sendo realizados em desacordo com o especificado, ou ainda que possa atentar contra o sigilo de informações, a segurança de pessoas ou bens da CONTRATANTE.

21.9. Os serviços rejeitados por terem sido considerados mal executados, deverão ser refeitos corretamente, com o tipo de execução aprovado pela fiscalização, arcando a CONTRATADA com os ônus decorrentes do fato;

21.10. As decisões e providências que ultrapassarem a competência do executor (es) do Contrato deverão ser autorizadas pela autoridade competente desta instituição em tempo hábil para a adoção das medidas pertinentes;

21.11. Exigir, quando couber, comprovação de que a CONTRATADA mantém reserva de cargos para pessoa com deficiência ou para reabilitado da Previdência Social, conforme disposto no art. 66-A da Lei nº 8.666, de 1993;

21.12. A CONTRATADA deverá manter preposto, aceito pela CONTRATANTE, durante o período de vigência do contrato, para representá-la sempre que for necessário.

22. DAS OBRIGAÇÕES DA CONTRATANTE

22.1. Permitir o acesso às suas dependências aos empregados da CONTRATADA para a entrega do objeto contratado.

22.2. Acompanhar e fiscalizar toda a execução do objeto, assegurando assim o cumprimento de todas as condições estabelecidas neste Termo de Referência.

22.3. Efetuar o pagamento à CONTRATADA conforme prazo e forma previstos neste Termo de Referência.

22.4. Solicitar, sempre que necessário, esclarecimentos à CONTRATADA quanto ao fornecimento do objeto, notificando-a por escrito quando identificadas irregularidades na sua execução ou quando apresentados problemas durante a vigência do período de garantia dos produtos e serviços.

22.5. Rejeitar, no todo ou em parte, objeto entregue fora das especificações técnicas exigidas.

22.6. Aplicar à CONTRATADA, quando necessário, as sanções legais cabíveis, garantida a ampla defesa.

23. DAS OBRIGAÇÕES DA CONTRATADA

23.1. A CONTRATADA deve cumprir todas as obrigações constantes no Termo de Referência, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da execução do objeto e, ainda:

23.1.1. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

23.1.2. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

23.1.3. Comunicar à CONTRATANTE, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

23.1.4. Manter, durante toda a contratação, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

23.1.5. Indicar preposto para representá-la durante a contratação.

23.1.6. Os serviços de link dedicado de internet deverão estar em conformidade com a proposta apresentada e nas quantidades especificadas;

23.1.7. No que se refere à utilização de postes da Companhia de Energia Elétrica para passagem das fibras ópticas, a autorização deve ser obtida pela CONTRATADA e apresentada para a Secretaria de Segurança Pública do Distrito Federal na pessoa da Subsecretaria de Modernização Tecnológica - SMT;

23.1.8. A execução dos serviços deverá ser efetuada por funcionários da empresa CONTRATADA ou de empresa terceirizada, sob responsabilidade da CONTRATADA, devidamente identificados com uniforme ou crachá e portando cédula de identidade;

23.1.9. A CONTRATADA fornecerá os materiais e os ativos de rede a serem utilizados para execução dos serviços;

23.1.10. Todos os dispositivos, acessórios, materiais, ferramentas e equipamentos essenciais ou complementares a execução dos serviços, são de responsabilidade da CONTRATADA;

23.1.11. A execução dos serviços deverá seguir todos os procedimentos de segurança, tanto para os funcionários, transeuntes e demais pessoas envolvidas no processo, bem como, as normas locais, estaduais e federais pertinentes.

23.1.12. A CONTRATADA deverá responsabilizar-se integralmente pelos serviços efetuados e, em pleno funcionamento;

23.1.13. No caso de impossibilidade da manutenção por falta de peças ou outro motivo de força maior, o problema deve ser especificado por meio de laudo técnico emitido pela CONTRATADA.

23.1.14. O laudo será analisado por profissional do Subsecretaria de Modernização Tecnológica - SMT que poderá ser aceito ou não.

23.1.15. As despesas decorrentes do transporte/deslocamento de técnicos, bem como de veículos, equipamentos e ferramentas necessárias para a execução dos serviços são de responsabilidade da CONTRATADA.

23.1.16. Ao término da execução de cada registro de chamada serão emitidos um laudo de certificação do serviço executado.

23.1.17. Um técnico da Subsecretaria de Modernização Tecnológica - SMT deverá realizar uma vistoria e emitir um Termo de Aceite.

23.1.18. Os serviços não aceitos deverão ser refeitos sem ônus para a CONTRATANTE, sempre que for constatado o emprego de material inadequado ou a execução imprópria do serviço, à vista das especificações respectivas, sem que disto resulte ainda atraso na execução dos demais serviços propostos.

23.1.19. A CONTRATADA poderá ser responsabilizada por qualquer prejuízo que venha causar ao GDF em virtude de ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ambientais ligadas à utilização de produtos na manutenção dos equipamentos a que se refere este Edital e seus anexos.

23.1.20. A CONTRATADA poderá ser responsabilizada por qualquer atraso ou problemas na execução dos serviços;

23.1.21. A CONTRATADA poderá responder por quaisquer acidentes de que possam ser vítimas seus empregados, quando em serviço.

23.1.22. A CONTRATADA deverá arcar com todos os custos para cumprimento da garantia, inclusive no caso de necessidade de transporte (técnicos ou equipamentos);

23.1.23. Executar o objeto contratado, conforme as condições prescritas no presente instrumento e de acordo com as especificações deste Termo de Referência.

23.1.24. Entregar o serviço constantes no presente contrato, em restrita obediência as especificações técnicas descritas nas condições estabelecidas

23.1.25. Comunicar aos Gestores do Contrato toda e qualquer situação anômala que possam causar prejuízos à Administração.

23.1.26. Comunicar expressamente à Secretaria de Segurança Pública do Distrito Federal na pessoa da Secretaria de Modernização Tecnológica, a quem competirá deliberar a respeito, toda e qualquer situação anômala no decorrer da execução do objeto da presente licitação.

23.1.27. Repor, no prazo máximo de 24 (vinte e quatro) horas apurado o dolo ou a culpa, qualquer objeto da Administração e/ou de terceiros que tenha sido danificado ou extraviado por seus empregados.

23.1.28. Prestar à Administração, sempre que necessário esclarecimento sobre o serviço, fornecendo toda e qualquer orientação solicitada.

23.1.29. A CONTRATADA será responsável por quaisquer danos, perdas ou avarias a que der causa, por si e/ou por seus empregados, em instalações, informações e/ou pertences à Administração ou de terceiros em decorrência de dolo ou culpa, seja por imprudência, negligência ou imperícia, respondendo pelo ressarcimento dos prejuízos apurados.

23.1.30. Atender aos encargos trabalhistas, previdenciários, fiscais e comerciais decorrentes da execução do presente contrato;

23.1.31. Apresentar, sempre que solicitado, durante a execução do Contrato, documentos que comprovem estar cumprindo a legislação em vigor quanto às obrigações assumidas na licitação, em especial, encargos sociais, trabalhistas, previdenciários, tributários, fiscais e comerciais.

24. DA OBRIGATORIEDADE DO USO DE CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

24.1. Em atenção à Lei nº 4.770/2012 serão exigidos neste certame a aplicação de critérios de sustentabilidade ambiental;

24.2. Em relação ao Fabricante, ao produtor ou ao fornecedor, conforme art. 1º, inc. I, da Lei nº 4.770/2012;

24.3. A contratada deverá aplicar como critérios de sustentabilidade ambiental para a execução do contrato:

24.3.1. A adoção de processos de extração, fabricação e utilização de produtos e matérias-primas de forma ambientalmente sustentável;

24.3.2. A deposição e o tratamento adequados de dejetos e resíduos da indústria, comércio ou construção civil, bem como da água utilizada;

24.3.3. A utilização de matéria-prima renovável, reciclável, biodegradável e atóxica;

24.3.4. A utilização de tecnologia e material que reduzam o impacto ambiental;

24.3.5. A logística reversa.

24.4. Em relação ao FORNECEDOR, conforme art. 2º, inc. I, da Lei nº 4.770/2012; a contratada deverá aplicar como critérios de sustentabilidade ambiental para a execução do contrato:

24.4.1. A recepção de bens, embalagens, recipientes ou equipamentos inservíveis e não reaproveitáveis por essa Administração pública;

24.4.2. A comprovação de que adota práticas de desfazimento sustentável, reciclagem dos bens inservíveis e processos de reutilização.

24.5. Conforme art. 7º, incisos I a VIII, da Lei nº 4.770/2012; a contratada deverá fornecer bens que, no todo ou em parte:

24.5.1. Sejam constituídos por material reciclado, atóxico e biodegradável, na forma das normas da Associação Brasileira de Normas Técnicas – ABNT;

24.5.2. Ofereçam menor impacto ambiental em relação aos seus similares;

24.5.3. Não contenham substâncias perigosas acima dos padrões tecnicamente recomendados por organismos nacionais ou internacionais;

24.5.4. Estejam acondicionados em embalagem adequada, feita com a utilização de material reciclável, com o menor volume possível;

24.5.5. Funcionem com baixo consumo de energia ou de água;

24.5.6. Sejam potencialmente menos agressivos ao meio ambiente ou que, em sua produção, signifiquem economia no consumo de recursos naturais;

24.5.7. Possuam certificado emitido pelos órgãos ambientais;

24.5.8. Possuam certificação de procedência de produtos.

24.6. A comprovação dos requisitos citados acima poderá ser realizada por apresentação de declaração própria ou de certificação emitida por instituição pública oficial ou instituição credenciada, ou qualquer outro meio de prova que ateste que comprove que ateste que o bem fornecido cumpre com as exigências de práticas de sustentabilidade ambiental, conforme art. 7º, Parágrafo único, da Lei Distrital nº 4.770/2012.

25. DA VIGÊNCIA DO CONTRATO

25.1. O prazo de vigência do contrato é de 36 (trinta e seis) meses, contados a partir da assinatura do contrato, prorrogável na forma da lei, persistindo as obrigações decorrentes da garantia;

25.2. A contratação dos fornecedores registrados será formalizada pela SSP/DF por intermédio de instrumento contratual, emissão de nota de empenho ou outro instrumento hábil, conforme determina o art. 62, da Lei nº 8.666/93;

25.3. O prazo para assinatura do contrato será de até 05 (cinco) dias úteis, contados a partir da intimação do adjudicatário, podendo ser prorrogado uma vez por igual período, desde que ocorra motivo justificado e aceito pela Administração.

26. DO SIGILO E CONFIDENCIALIDADE DE INFORMAÇÕES

26.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos.

26.2. O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade CONTRATANTE, a ser assinado pelo representante legal da Contratada, e Termo de Ciência, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se no Anexo VII - Termo de Sigilo e Confidencialidade e Anexo VIII - Termo de Ciência.

27. DO RECEBIMENTO E CRITÉRIO DE ACEITAÇÃO DO SERVIÇO

27.1. O serviço deverá ser entregue conforme disposto neste item.

27.2. Será recebido o serviço:

27.3. Provisoriamente, pelo responsável por seu acompanhamento e fiscalização, mediante termo circunstanciado, assinado pelas partes em até 15 (quinze) dias da comunicação escrita do contratado;

27.3.1. Definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo de observação, ou vistoria que comprove a adequação do objeto aos termos contratuais, observado o disposto no art. 69 da Lei nº 8.666/1993;

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

27.3.3. 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.

27.3.4. Se a licitante vencedora deixar de entregar o serviço dentro do prazo estabelecido sem justificativa por escrito, aceita pela Administração, sujeitar-se-á às penalidades impostas no Decreto n° 26.851/2006, e suas alterações posteriores (Decretos nº 26.993/2006, nº 27.069/2006, nº 35.831 e nº 36.974/2015), na Lei Federal n° 8.666/1993 e alterações subsequentes, no Edital e neste Termo de Referência.

27.4. A Contratante poderá a seu exclusivo critério, por conveniência administrativa, dispensar o recebimento provisório dos serviços, nos termos do artigo 74, inciso II, da Lei nº 8.666/1993.

28. DO ACOMPANHAMENTO E FISCALIZAÇÃO

28.1. O Executor e/ou Comissão designada do contrato anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário a regularização das faltas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

28.2. O executor e/ou comissão executora, durante seu mister, deve agir de forma pró-ativa e preventiva, observar o cumprimento pela contratada das regras previstas no instrumento contratual, buscar os resultados esperados no ajuste e trazer benefícios e economia para esta Secretaria, devendo cumprir integralmente a PORTARIA Nº 119-SSP, que estabelece diretrizes para a gestão, acompanhamento e fiscalização da execução de contratos, convênios, acordos e instrumentos congêneres celebrados pela SSP.

28.3. O executor ou comissão de execução do contrato deverá informar à Autoridade Máxima do setor requisitante do contrato, com antecedência mínima de 12 meses do término do prazo previsto no inciso II, do artigo 57, da Lei nº 8.666/93, quando se tratar de prestação de serviços contínuo.

28.4. 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 do executor do contrato especificamente designado, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, podendo:

28.4.1. Sustar a execução de qualquer trabalho que esteja sendo feito em desacordo com o especificado, sempre que essa medida se torne necessária;

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

28.4.3. Determinar a reexecução dos serviços realizados com falha, erro ou negligência, lavrando termo de ocorrência do evento.

28.5. Além das disposições acima citadas, a fiscalização administrativa deverá observar, ainda, as seguintes diretrizes:

a) Fiscalização mensal (a ser feita antes do pagamento da fatura):

b) Deve ser feita a retenção da contribuição previdenciária no valor de 11% (onze por cento) sobre o valor da fatura e dos impostos incidentes sobre a prestação do serviço.

c) Deve ser consultada a situação da empresa junto ao SICAF.

d) Serão exigidos a Certidão Negativa de Débito (CND) relativa a Créditos Tributários Federais e à Dívida Ativa da União, o Certificado de Regularidade do FGTS (CRF) e a Certidão Negativa de Débitos Trabalhistas (CNDT), caso esses documentos não estejam regularizados no SICAF.

e) Exigir, quando couber, comprovação de que a empresa mantém reserva de cargos para pessoa com deficiência ou para reabilitado da Previdência Social, conforme disposto no art. 66-A da Lei nº 8.666, de 1993.

29. DO PAGAMENTO E ADEQUAÇÃO ORÇAMENTÁRIA

29.1. Há previsão orçamentária para a realização da despesa, a qual correrá à conta de recursos específicos;

29.2. A Coordenação de Orçamento, Finanças, Contratos, Convênios e Fundos, da Subsecretaria de Administração Geral, indicará o Programa de Trabalho, a Fonte, a Natureza de Despesa, o código de subatividade e demais informações atinentes à classificação orçamentária das despesas decorrentes;

29.3. Para efeito de pagamento, a Contratada deverá apresentar os documentos abaixo relacionados, caso não estejam regularizados no SICAF:

29.4. Certidão Negativa ou Positiva com Efeito de Negativa de Débitos Relativos todos os créditos tributários federais e à Dívida Ativa da União e créditos tributários relativos, expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), conforme Portaria Conjunta RFB-PGFN nº 1.751/2014, alterada pela Portaria Conjunta RFB-PGFN nº 3.193/2017;

29.5. Certificado de Regularidade do Fundo de Garantia por Tempo de Serviço – FGTS, fornecido pela CEF – Caixa Econômica Federal, devidamente atualizado (Lei nº 8.036/1990);

29.6. Certidão Negativa ou Positiva com Efeito de Negativa de Débitos Trabalhistas (CNDT), em plena validade e expedida pelo Tribunal Superior do Trabalho, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

29.7. A Contratada deverá apresentar a Certidão Negativa ou Positiva, com Efeito de Negativa, que comprove a Regularidade junto à Fazenda do Distrito Federal.

29.8. O pagamento decorrente da Contratação deverá ser efetuado em até 30 (trinta) dias, contados a partir da data de apresentação da Nota Fiscal, devidamente atestada pelo Gestor do Contrato, desde que o documento de cobrança esteja em condições de liquidação e pagamento, mediante crédito em conta corrente em nome da contratada, seguindo as disposições contidas nas Normas de Planejamento, Orçamento, Finanças, Patrimônio e Contabilidade do Distrito Federal;

29.9. 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 com a variação **"*pro rata tempore*"**, do Índice Nacional de Preços ao Consumidor Amplo (IPCA), em conformidade com o disposto no art. 2º do Decreto distrital nº 37.121/2016;

29.10. Nenhum pagamento será efetuado à contratada enquanto pendente de liquidação qualquer obrigação que lhe for imposta em virtude de penalidade ou inadimplência;

29.11. O atraso do pagamento, em virtude de penalidade e/ou inadimplência da Contratada, não gerará direito de reajuste de preços ou de correção monetária;

29.12. Caso haja multa por inadimplemento contratual, será adotado o seguinte procedimento:

29.13. Se o valor da multa for superior ao valor da garantia prestada, além da perda desta, responderá o contratado por sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Administração, ou ainda, quando for o caso, cobrada judicialmente;

29.14. A multa será formalizada por simples apostilamento contratual, na forma prevista no art. 65, §8°, da Lei nº 8.666/1993, e será executada após regular processo administrativo, oferecido à contratada o direito 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 8.666/1993;

29.15. Para as empresas com sede ou domicílio no Distrito Federal, com créditos de valores iguais ou superiores a R$5.000,00 (cinco mil reais), os pagamentos serão 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 agência onde deseja receber seus créditos, de acordo com o Decreto nº 32.767/2011, publicado no DODF nº 35, de

18/02/2011.

29.16. A regra definida no Decreto nº 32.767/2011, não se aplica:

29.16.1. aos pagamentos a empresas vinculadas ou supervisionadas pela Administração Pública Federal;

29.16.2. aos pagamentos efetuados à conta de recursos originados de acordos, convênios ou contratos que, em virtude de legislação própria, só possam ser movimentados em instituições bancárias indicadas nos respectivos documentos; e

29.16.3. aos pagamentos a empresas de outros Estados da federação que não mantenham filiais e/ ou representações no DF e que venceram processo licitatório no âmbito deste ente federado. (Art. 6º c/c 7º do Decreto distrital nº 32.767/2011).

29.17. Por ocasião do pagamento será feita a retenção do Imposto de Renda incidente sobre os serviços prestados, conforme estabelece a Portaria nº 247/2019 - Secretaria de Estado de Economia do Distrito Federal (SEEC/DF).

Do Reajuste Contratual

29.18. Em caso de reajuste de preços por aplicação de índice de correção monetária será adotado o Índice Nacional de Preços ao Consumidor-IPCA, apurado pelo Instituto Brasileiro de Geografia e Estatística-IBGE, de acordo com o Decreto 37.121, de 16 de fevereiro de 2016, que dispõe sobre a racionalização e o controle de despesas públicas no âmbito do Governo do Distrito Federal.

30. DAS PENALIDADES

30.1. Pelo descumprimento de quaisquer das obrigações assumidas, mora ou inexecução parcial ou total, serão aplicadas as penalidades estabelecidas no Decreto 26.851/2006 e alterações, e as demais previstas nas Leis Federais 8.666/93 e 10.520/2002, sem prejuízo da consonância com o que estiver previsto no Edital do Pregão e nos itens que seguem;

30.2. Aquele que, convocado dentro do prazo de validade de sua proposta, não assinar o contrato, recusar-se a aceitar a nota de empenho, deixar de entregar documentação exigida no Edital, apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, ou se enquadrar em qualquer tipo previsto nas legislações vigentes, que prejudique de qualquer forma a Administração Pública, garantido o direito à ampla defesa, ficará impedido de licitar e de contratar com o Distrito Federal pelo prazo de até cinco anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais;

30.3. 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 n.ºs 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:

30.3.1. Será notificada formalmente em caso de descumprimento de obrigação contratual e terá que apresentar as devidas justificativas em um prazo de até 5 (cinco) dias úteis após o recebimento da notificação. Caso não haja manifestação dentro desse prazo ou esta seja entendida como improcedente, a CONTRATADA será advertida;

30.3.2. Multa, conforme percentuais definido no Decreto nº 26.851 e suas atualizações;

30.3.3. 0,1% por dia, no caso de descumprimento do prazo de implantação, calculado sobre o valor dos produtos adjudicados, limitada a incidência a 30 (trinta) dias de atraso;

30.3.4. No caso de atraso injustificado na entrega do objeto por prazo superior a 30 (trinta) dias, com a aceitação do objeto pela Administração, será aplicada multa de 15% (quinze) sobre o valor dos produtos adjudicados;

30.3.5. No caso de atraso injustificado na entrega dos objetos por prazo superior a 30 (trinta) dias, com a não aceitação do objeto pela Administração, caracterizando-se nesta hipótese a inexecução total da obrigação;

30.3.6. Multa de 2% (dois por cento) sobre o valor total da nota fiscal do serviço prestado no mês, no caso de descumprimento para o início de atendimento, limitado a cinco chamados por período;

30.3.7. Multa de 5% (cinco por cento) sobre o valor total da nota fiscal do serviço prestado no mês, no caso de descumprimento para o início de atendimento presencial, limitado a cinco ocorrências por período;

30.3.8. Multa de 5% (cinco por cento) sobre o valor total da nota fiscal do serviço prestado no mês, no caso da interrupção do atendimento do chamado sem notificação prévia à CONTRATANTE, limitado a cinco ocorrências por período;

30.3.9. A reincidência em mais de um mês do descumprimento dos níveis de serviço relacionados ao atendimento de 5 (cinco) chamados, para as sanções previstas, com a não aceitação do objeto pela Administração, caracterizando-se nesta hipótese a inexecução total da obrigação;

30.3.10. Multa de 10% (dez por cento) sobre o valor total adjudicado, no caso de inexecução parcial da obrigação assumida;

30.3.11. Multa de 20% (vinte por cento) sobre o valor total adjudicado, no caso de inexecução total da obrigação;

30.3.12. 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;

30.3.13. 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.

30.4. 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;

30.4.1. As multas serão descontadas dos pagamentos a que a CONTRATADA fizer jus no prazo de quinze dias corridos, contados a partir da data da comunicação, ou ainda, quando for o caso, descontados da Garantia Contratual ou cobradas judicialmente;

30.4.2. Para a aplicação das penalidades aqui previstas, a CONTRATADA será notificada para apresentar defesa prévia, no prazo de cinco dias úteis, contados a partir do recebimento da notificação;

30.4.3. As penalidades previstas no contrato são independentes entre si, podendo ser aplicadas isolada ou cumulativamente, sem prejuízo de outras medidas cabíveis;

30.4.4. As licitantes e/ou CONTRATADAS deverão cumprir as determinações do DECRETO Nº 39.860, DE 30 DE MAIO DE 2019, que dispõe sobre a proibição de participação, direta ou indiretamente, de licitação, contratação, execução de obra ou serviço e do fornecimento de bens a eles necessários agentes públicos de órgãos ou entidades da Administração Pública Direta ou Indireta do Poder Executivo do Distrito Federal CONTRATANTE ou responsável pela licitação, sob pena de responsabilização nos âmbitos administrativo e judicial.

30.4.5. A aplicação de penalidades, inclusive o pagamento de eventuais multas, previstas no contrato não exime a CONTRATADA da reparação de eventuais danos, perdas ou prejuízos que vier a causar à CONTRATANTE.

31. DOS RESPONSÁVEIS PELA ELABORAÇÃO DO DOCUMENTO

31.1. Vossa apreciação com a informação que o presente Termo foi elaborado e ajustado pela Equipe de Planejamento da Contratação, instituída por meio do meio dos Despachos 100343432, 79606748 e 116303197, para atender a legislação vigente.

INTEGRANTE REQUISITANTE	INTEGRANTE TÉCNICO	INTEGRANTE TÉCNICO	INTEGRANTE ADMINISTRATIVO
HÉLIO DE FARIAS SOARES Matrícula nº 1.713.991-0	**DOUGLAS WILLIAN BARBOSA MOREIRA** Matrícula nº 1.699.997-5	**GLÁUCIO SILVEIRA E SILVA** Matrícula nº 1.691.710-3	**MAXWELL AMÉRICO MARINELLO** Matrícula nº 1.698.5885-3

AUTORIDADE MÁXIMA DA ÁREA DE TIC
FÁBIO MARTINS DA SILVA Subsecretário de Modernização Tecnológica Matrícula nº 1.712.453-0

32. ANEXOS

32.1. O presente Termo de Referência é composto dos seguintes anexos:

32.1.1. **Anexo I** - Termo de Recebimento Provisório;

32.1.2. **Anexo II** - Termo de Recebimento Definitivo;

32.1.3. **Anexo III** - Modelo de Proposta;

32.1.4. **Anexo VI** - Ordem de Serviço;

32.1.5. **Anexo V** - Relatório de Vistoria Técnica;

32.1.6. **Anexo VI** - Declaração de Desistência da Vistoria;

32.1.7. **Anexo VII** - Termo de Sigilo e Confidencialidade;

32.1.8. **Anexo VIII** - Termo de Ciência;

ANEXO I - TERMO DE RECEBIMENTO PROVISÓRIO

À Secretaria de Estado da Segurança Pública do Distrito Federal SSP/DF
SAM Conjunto A Bloco A
Setor de Administração Municipal , Sede da SSP/DF - Asa Norte
CEP: 70620–000- Brasília, DF

OBJETO:	
N. º CONTRATO:	
N.° da OS:	
CONTRATADA:	

CNPJ:	
TELEFONE (S):	

Por este instrumento, atestamos para fins de cumprimento do disposto no Art. 73, inciso II, alínea “a”, da Lei nº 8.666, de 21 de junho de 1993, que os bens e/ou serviços, relacionados no quadro abaixo, foram recebidos nesta data e serão objeto de avaliação quanto aos aspectos de qualidade, de acordo com os Critérios de Aceitação previamente definidos pelo Edital de Pregão Eletrônico SRP n.º xx/20xx da SSP/DF.

Item	Descrição	Identificação	Unidade	Quantidade

Ressaltamos que o recebimento definitivo dos bens e/ou serviços ocorrerá em até 15 (quinze) dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do instrumento contratual proveniente do Edital de Pregão Eletrônico SRP n° xx/20xx.

Brasília, de de 20___.

_____

SERVIDOR

CARGO

Matrícula

ANEXO II - TERMO DE RECEBIMENTO DEFINITIVO

À Secretaria de Estado da Segurança Pública do Distrito Federal SSP/DF

SAM Conjunto A Bloco A

Setor de Administração Municipal , Sede da SSP/DF - Asa Norte

CEP: 70620–000- Brasília, DF

OBJETO:	
N. º CONTRATO:	
N.° da OS:	
CONTRATADA:	
CNPJ:	
TELEFONE (S):	

Por este instrumento, as partes abaixo identificadas atestam para fins de cumprimento do disposto no Art. 73, inciso II, alínea “b”, da Lei nº 8.666, de 21 de junho de 1993, que os bens e/ou serviços relacionados no quadro abaixo, possuem as quantidades, configuração, desempenho e a qualidade compatível com as condições e exigências técnicas constantes do Edital n° xx/20xx.

Item	Descrição	Identificação	Unidade	Quantidade

Brasília, de de 20___.

_____

EXECUTOR DO CONTRATO

CARGO

Matrícula

_____

REPRESENTANTE DA ÁREA

REQUISITANTE DA SOLUÇÃO

CARGO

Matrícula

ANEXO III - MODELO DE PROPOSTA

À Secretaria de Estado da Segurança Pública do Distrito Federal SSP/DF

SAM Conjunto A Bloco A

Setor de Administração Municipal , Sede da SSP/DF - Asa Norte

CEP: 70620–000- Brasília, DF

Local e data

Referência: Edital do Pregão Eletrônico Nº ____/2021 – SSPDF

Sr. Pregoeiro,

A Empresa _____ sediada à (rua, bairro, cidade), Telefone_____, inscrita no CNPJ/MF sob nº _____, neste ato representada por_____, abaixo assinada, propõe à SSPDF, o fornecimento dos materiais abaixo indicado(s), conforme Termo de Referência do Edital em epígrafe, nas seguintes condições:

GRUPO	ITEM	ESPECIFICAÇÃO MÍNIMA ACEITÁVEL	U.N.	QUANTIDADE	VALOR DE REFERÊNCIA UNITÁRIO	VALOR DE REFERÊNCIA TOTAL
1	1	Tipo I - Firewall de alta capacidade, destinados a segurança de data center	Unidade	2	R$	**R$**
	2	Tipo II - Firewall intermediário destinado as localidades WAN	Unidade	3		
	3	Sistema de gerenciamento e processamento de logs.	Unidade	1		

2	**4**	Solução de antivírus com licenciamento perpétuo, para estação de trabalho.	Unidade	500		
	5	Solução de antivírus com licenciamento perpétuo, para equipamentos servidores.	Unidade	300		
	TOTAL:				**R$**	

Valor total da proposta R$ _____._____,___ (_____) em algarismos e por extenso.

- Nos preços acima estão incluídos todos os insumos que compõem o objeto, inclusive as despesas com impostos, taxas, frete, seguros, garantia estendida e quaisquer outros que incidam direta ou indiretamente no fornecimento dos materiais;

- Prazo de entrega dos materiais: **60 (sessenta) dias úteis a contar da assinatura do contrato ou do recebimento da nota de empenho;**

- Garantia de fábrica;

- Garantia estendida (quando houver);

- A entrega dos materiais será feita no local determinado pela SSPDF, sem nenhum ônus para a CONTRATANTE;

- Prazo de validade da proposta: (deverá ser no mínimo de 90 dias);

- Dados bancários: (informar banco, agência e conta-corrente);

- Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Edital e seus anexos.

- Declaração de inclusão no portifólio atualizado do Fabricante dos equipamentos ofertados.

- Declaração de integração dos componentes dos equipamentos ofertados serão entregues mediante fiscalização da Contratante e Contratada.

- Declaração de inclusão de todos os tributos, fretes, tarifas e demais despesas decorrentes da execução do objeto.

_____
Nome , Cargo e Identidade do Representante da Empresa

Declaração de atendimento integral aos requisitos técnicos.

- Deverá ser anexado à proposta uma tabela como a inserida abaixo, relacionado todos os datasheets e descritivos técnicos, lembrando que links quebrados e referências indiretas ou subjetivas não serão aceitos, cabendo à equipe técnica promover diligências junto a proponente com o fito de sanar o erro; cada item deverá possuir uma referência à proposta ou datasheet que permita a equipe de contratação validar diretamente os itens.
- A empresa não poderá colocar somente o modelo do equipamento, mas deverá indicar onde e exatamente em que ponto do documento se localiza cada informação exigida no edital. Com a ressalva dos itens pedidos que podem ser conectados à solução, como cabos, transceivers, conectores e outros.

Itens do Edital	**Descrição**	Documento que condizem com a página referenciada ou sítio eletrônico/LINK comprovando o atendimento do respectivo item.
	Especificação Técnica - GRUPO 1	
	CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE FIREWALL	
	Os equipamentos devem ser mantidos atualizados na última versão de sistema operacional disponível pelo fabricante durante o período de vigência contratual; Os equipamentos devem ser do mesmo fabricante da solução de gerenciamento centralizado de logs; Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/ transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/ transceptores necessários para a plena utilização; A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP. Possuir 1 (uma) interface do tipo console ou similar; Possuir 1 (uma) interface de rede dedicada ao gerenciamento; Possuir fonte de alimentação redundante e hot-swappable; Possuir, no mínimo, 8 (oito) interfaces de rede 10 Gbps SFP+; Possuir, no mínimo, 16 (dezesseis) interfaces de rede 1Gbps UTP; Armazenamento de, no mínimo, 02 (dois) Solid State Drive (SSD) de 240 GB; Throughput de, no mínimo, 9.8 Gbps, para conexões VPN; Suporte a, no mínimo, 232.000 (duzentos e trinta e dois mil) novas conexões ou sessões por segundo; Suporte a, no mínimo, 12.000.000 (doze milhões) de conexões ou sessões simultâneas; Throughput de, no mínimo, 15 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;	
	É permitida a composição da solução ofertada dentro do mesmo fabricante, sendo vedada solução de software livre; A solução devera ser compatível com SMPv2 e SMPv3; Os Appliances devem permitir acesso ao equipamento via interface de linha de comando (CLI), console, SSH além de interface web HTTPS; Devem ser capazes de criptografar e autenticar a comunicação com a solução de gerenciamento centralizado e/ou de orquestração; Devem ser capazes de bloquear sessões TCP que utilizarem variações do 3-way handshake, como 4-way e 5-way split handshake, de modo a prevenir possíveis tráfegos maliciosos; As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos do mesmo fabricante, desde que obedeçam a todos os requisitos desta especificação; A comunicação entre os appliances de segurança e o módulo de gerência deve ser por meio criptografado; Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais; Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior data da proposta; Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital. A solução deve suportar a possibilidade de manutenção dinâmica de um equipamento de um cluster para outro, de acordo com a necessidade da arquitetura definida, sem que haja a perda do tráfego; A solução de balanceamento deverá ser fornecida em appliances físicos. A solução de balanceamento deverá ser fornecida em Alta Disponibilidade do tipo Ativo/Ativo; Os appliances deverão vir acompanhados de todos os conectores, cabeamento e peças de fixação no Rack, necessários à sua instalação e funcionamento, conforme as especificações deste Estudo Técnico Preliminar. Deve prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção; A solução deverá ser provida de forma redundante, de modo que se houver a falha de uma delas, a outra possa assumir totalmente o controle, sem que haja perda do tráfego; A solução deverá ser capaz de organizar os appliances de NG Firewall em grupos de segurança, nos quais os appliances de NG Firewall atuarão com seus recursos somados; A solução deverá ser capaz de suportar, no mínimo, 4 (quatro) grupos de segurança; A solução deverá possuir a quantidade de transceptores suficientes para conectar toda a solução à rede corporativa, o que inclui a gerência.	
	SOLUÇÃO EDR Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação: No mínimo, 2 interfaces 1000Base-T com conectores RJ-45; Discos redundantes com espaço de armazenamento para LOGs de pelo menos 8TB; Possuir fonte de energia AC redundante com ajuste automático de tensão para operação nas tensões de 100 a 240-VAC/60 Hz; Ser fornecido com todos os acessórios necessários para sua instalação;	
	REQUISITOS GERAIS DE SOFTWARE: A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7; O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta; Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM, IGMP), DHCP Relay, DHCP Server e Jumbo Frames; Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM); Deve suportar, no mínimo, roteamento BGP, OSPFv2, RIPv2 e roteamento estático; Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay; Os dispositivos de proteção de rede devem possuir suporte a DHCP Server; Os dispositivos de proteção de rede devem possuir suporte a DHCP Server no protocolo IPv6; Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas; Deve suportar NAT dinâmico (Many-to-Many); Deve suportar NAT estático (1-to-1); Deve suportar NAT estático bidirecional 1-to-1; Deve suportar Tradução de porta (PAT); Deve suportar NAT de Origem; Deve suportar NAT de Destino; Deve suportar NAT de Origem e NAT de Destino simultaneamente; Deve implementar Network Prefix Translation (NPTv6) ou NAT66 (IPv6-to-IPv6), prevenindo problemas de roteamento assimétrico; Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco e situação do cluster; Enviar log para sistemas de monitoração externos; Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL; Proteção anti-spoofing; Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego; Suporte a configuração de alta disponibilidade (HA) Ativo/Passivo e Ativo/Ativo. Caso o suporte à configuração de alta disponibilidade (HA) implique em algum licenciamento adicional que aumente o valor da proposta esta funcionalidade não deverá ser incluída nos equipamentos do Grupo II;	

	A configuração em alta disponibilidade (HA) deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB; O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link; Suportar cluster para alta-disponibilidade do tipo ativo-ativo, permitindo que um cluster possa realizar o load balance das sessões para inspeção profunda sem a necessidade de implementações ou mudanças na rede ou nos terminais já existentes; Controle, inspeção e descriptografia de SSL para tráfego de Saída (Outbound); Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos; Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. 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. **POLÍTICAS:** Deverá suportar controles por zonas de segurança; Deverá suportar controles de políticas por porta e protocolo; Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações; Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança; Controle de políticas por nome ou código de País (Por exemplo: BR, US, UK, RU);3.1.7.6. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound); Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3; Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada; Suporte a objetos e regras IPV6; Suporte a objetos e regras multicast; Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários e datas pré-definidos automaticamente. NAT64 e NAT46.	
	CONTROLE DE APLICAÇÕES: Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo; Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos; Reconhecer pelo menos 3.000 (três mil) aplicações diferentes, incluindo, mas não limitado: a 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; 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, onedrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs; Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo; 3.1.8.6. 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 utilização da rede Tor; Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante; Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação; Identificar o uso de táticas evasivas via comunicações criptografadas; Atualizar a base de assinaturas de aplicações automaticamente; Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários; Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras; Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos; Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante; O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações; Deve alertar o usuário quando uma aplicação for bloqueada; Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos; Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts,Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos; Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo; Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos; Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (ClientServer, Browse Based, Network Protocol, etc); Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação; Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.	
	PREVENÇÃO DE AMEAÇAS: Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall; Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware); Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade; Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: Permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo; As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração; Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança; Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura; Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens; Deve permitir o bloqueio de vulnerabilidades; Deve permitir o bloqueio de exploits conhecidos; Deve incluir proteção contra-ataques de negação de serviços; Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc; Detectar e bloquear a origem de portscans; Bloquear ataques efetuados por worms conhecidos; Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS; Possuir assinaturas para bloqueio de ataques de buffer overflow; Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto; Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações; Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMTP e POP3; Identificar e bloquear comunicação com botnets; Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo; Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas; Os eventos devem identificar o país de onde partiu a ameaça; Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms; Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos; Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários,origem, destino, zonas de segurança, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos; Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back; A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;	
	FILTRO DE URLS: 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); Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança; Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório,Active Directory e base de dados local; A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall; Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL; Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo; Possuir pelo menos 70 categorias de URLs; Deve possuir a função de exclusão de URLs do bloqueio; Permitir a customização de página de bloqueio; Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;	
	IDENTIFICAÇÃO DE USUÁRIOS: 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; Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários; Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2018; Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários; Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários; Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários; Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal); 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; Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD; Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP); A solução deve suportar nativamente a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X;	
	FILTRO DE DADOS: Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc); Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;	

	Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos; 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.	
	GEOLOCALIZAÇÃO: Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados; Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;	
	VPN: Suportar VPN IPSec Site-to-Site; A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard); A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512; A VPN IPSEc deve suportar no mínimo Diffie-Hellman Group 1, Group 2, Group 5; A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2); A VPN IPSEc deve suportar Autenticação via certificado IKE PKI; Deve possuir integração com Amazon, AWS, Google Cloud, IBM Cloud VPC, Kubernetes, Azure a fim de permitir a criação de objetos dinâmicos com base nos endereços IPs das instancias virtuais na nuvem; O cliente VPN deve suportar autenticação via SAML 2.0 a fim de permitir integração com plataformas Azure AD, Google Authentication ou outro provedor de identidade; O cliente de VPN deve estar disponível na loja de aplicativos AppStore e PlayStore;	
	SD-WAN: Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação; As funcionalidades de segurança e SD-WAN que compõem a solução devem funcionar em equipamento único obedecendo a todos os requisitos desta especificação; A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação; Deve ser possível criar políticas para modelagem do tráfego definido pelo menos os parâmetros: IP de origem; Grupo de usuário VLAN de origem; IP de destino; Porta TCP/UDP de destino; Domínio e URL de destino; Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox); A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp; O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente; O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade e realizar a reordenação dos pacotes desse mesmo fluxo no outro extremo; Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo; A solução deve permitir a definição do roteamento para cada aplicação; Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis mínimos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação; Deve possibilitar a definição do link de saída para uma aplicação específica; Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, dois links; Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais; A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding; Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF); Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos; Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões; Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido; Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar: Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;	
	DAS FUNCIONALIDADES DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB A solução devera contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL; Controle de políticas por usuários, grupos de usuários, IPs e redes; Deve de-criptografar trafego de entrada e saída em conexões negociadas com TLS 1.2; Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação; Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente; Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades: Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos; Reconhecer pelo menos 3.000 (Três mil) aplicações diferentes, incluindo, mas não limitado: a trafego 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; Para trafego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas; A solução deve suportar a recategorização de URLs local; Atualizar a base de assinaturas de aplicações automaticamente; A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante; Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDCP/CD; Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários; Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou analise heurística; Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão; A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL: Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora); Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes; Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL; Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário; Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre; Suportar a criação de categorias de URLs customizadas; Permitir a customização de pagina de bloqueio; Como melhor prática do uso do acesso a internet e respeitando as políticas de segurança do orgão, a ferramenta deve criar uma página customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma pagina URL ou aplicação WEB de acordo com as políticas de acesso estabelecidas pela área de TI; Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários; Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal); A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos: PCI – números de cartão de crédito; Arquivos PDF; Arquivos executáveis; Arquivos de banco de dados; Arquivos do tipo documento; Arquivos do tipo apresentação; Arquivos do tipo planilha; A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload"; A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma pagina web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito; A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes sendo trafegados pela Web em paginas utilizando o protocolo HTTPS.	
	DAS FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti- Malware integrados no próprio equipamento de firewall; Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos; A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo; A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo; Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens; A solução de IPS deve possuir análise de padrões de estado de conexões, analise de decodificação de protocolo, analise para detecção de anomalias de protocolo, remontagem de pacotes de TIP e bloqueio de pacotes malformados; Detectar e bloquear a origem de portscans; Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações; A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT; Possuir assinaturas para bloqueio de ataques de buffer overflow; Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP; Suportar bloqueio de arquivos por tipo; Identificar e bloquear comunicação com botnets; Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção; Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e AntiMalware, através da console de gerência centralizada;	

	Os eventos devem identificar o país de onde partiu a ameaça; Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.); Possuir a capacidade de prevenção de ameaças não conhecidas; Suportar a criação de políticas por Geo-Localização, permitindo que o trafego de determinado País/Países seja bloqueado; Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos; A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;	
	DAS FUNCIONALIDADES E CONTROLE DE QUALIDADE DE SERVIÇO Suportar a criação de políticas de QoS por: Endereço de origem, endereço de destino e por porta; O QoS deve possibilitar a definição de classes por: Banda garantida; Banda máxima ; Fila de prioridade; Disponibilizar estatisticas RealTime para classes de QoS;	
	DAS FUNCIONALIDADES DE VPN Suportar VPN Site-to-Site e Cliente-To-Site; Suportar IPSec VPN; Suportar SSL VPN; A VPN IPSEc deve suportar: 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI; A solução deve suportar CA Interna e CA Externa de terceiros; A Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);	
	GERENCIAMENTO CENTRALIZADO DE LOGS E RELATÓRIOS Os equipamentos devem ser mantidos atualizados na última versão de sistema operacional disponível pelo fabricante durante o período de vigência contratual; Os equipamentos devem ser do mesmo fabricante da solução de firewall; Deve fornecer throughput mínimo de 25 GB/dia de Logs; Deve possuir capacidade de armazenamento de no mínimo 10TB; Deve possibilitar o envio/backup dos logs para um servidor de logs; Monitorar todo o tráfego e atividade da rede de dados da SSPDF, inclusive o tráfego e comunicação com a internet e redes externas; Apresentar histórico e fornecer relatórios das atividades realizadas na administração e operação da solução, bem como de todo o tráfego controlado e monitorado pela mesma; Deve permitir relatórios customizados na solução; Deve permitir geração de relatórios agendados ou sob demanda; Deve possuir relatórios pré-definidos na solução; Deve possuir console única de gerenciamento; Suporte a hypervisor VMware ESX/ESXi 5.5/6.0/6.5/6.7/7.0, no mínimo	
	DA SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS - EDR A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo CPT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa análise executada na nuvem proprietária da próprio fabricante ou appliance dedicada para sandboxing; Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTC durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente; A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL; A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016; Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização; A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTC) e Mirror/TAP; A tecnologia de máquina virtual devera possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas; A solução de prevenção de ameaças avançadas (Sandboxing) contra ataques persistentes e ZeroDay, deve ser habilitada e funcionar de forma independente, ou seja, não sendo obrigatório o uso e ativação de funcionalidades ou engines de anti-vírus para a mesma ter o seu devido funcionamento; Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante; Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb; Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP; Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. a solução deve permitir a analise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm; A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo; Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração: Quantidade de arquivos que estão em emulação; Número de arquivos emulados; A solução deve possuir os indicadores abaixo referente ao ultimo dia, ultima semana ou últimos 30 dias: Arquivos scaneados; Arquivos maliciosos;	
	GERENCIAMENTO DE LOG	
	Os equipamentos devem ser mantidos atualizados na última versão de sistema operacional disponível pelo fabricante durante o período de vigência contratual; Os equipamentos devem ser do mesmo fabricante da solução de firewall; Deve fornecer throughput mínimo de 25 GB/dia de Logs; Deve possuir capacidade de armazenamento de no mínimo 10TB; Deve possibilitar o envio/backup dos logs para um servidor de logs; Monitorar todo o tráfego e atividade da rede de dados da SSPDF, inclusive o tráfego e comunicação com a internet e redes externas; Apresentar histórico e fornecer relatórios das atividades realizadas na administração e operação da solução, bem como de todo o tráfego controlado e monitorado pela mesma; Deve permitir relatórios customizados na solução; Deve permitir geração de relatórios agendados ou sob demanda; Deve possuir relatórios pré-definidos na solução; Deve possuir console única de gerenciamento; Suporte a hypervisor VMware ESX/ESXi 5.5/6.0/6.5/6.7/7.0, no mínimo.	
	TIPO I - FIREWALL DE ALTA CAPACIDADE PARA SEGURANÇA DE DATA CENTER:	
	Os equipamentos devem ser mantidos atualizados na última versão de sistema operacional disponível pelo fabricante durante o período de vigência contratual; Os equipamentos devem ser do mesmo fabricante da solução de gerenciamento centralizado de logs; Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/ transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/ transceptores necessários para a plena utilização; A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP. Possuir 1 (uma) interface do tipo console ou similar; Possuir 1 (uma) interface de rede dedicada ao gerenciamento; Possuir fonte de alimentação redundante e hot-swappable; Possuir, no mínimo, 8 (oito) interfaces de rede 10 Gbps SFP+; Possuir, no mínimo, 16 (dezesseis) interfaces de rede 1Gbps UTP; Armazenamento de, no mínimo, 02 (dois) Solid State Drive (SSD) de 240 GB; Throughput de, no mínimo, 9.8 Gbps, para conexões VPN; Suporte a, no mínimo, 232.000 (duzentos e trinta e dois mil) novas conexões ou sessões por segundo; Suporte a, no mínimo, 12.000.000 (doze milhões) de conexões ou sessões simultâneas; Throughput de, no mínimo, 15 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;	
	TIPO II - FIREWALL INTERMEDIÁRIO: (DESTINADOS A LOCALIDADES WAN: SUDEC, GETRAM E NUAL.)	
	Os equipamentos devem ser mantidos atualizados na última versão de sistema operacional disponível pelo fabricante durante o período de vigência contratual; Os equipamentos devem ser do mesmo fabricante da solução de gerenciamento centralizado de logs; Throughput de, no mínimo, 800 (oitocentos) Mbps com a funcionalidade de Threat Prevention, ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Antivírus habilitadas; Throughput de, no mínimo, 6 (seis) Gbps de VPN IPSec; Estar licenciada para ou suportar sem o uso de licença de, no mínimo, 200 (duzentos) clientes de VPN SSL simultâneos; Estar licenciado para, ou suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos Suportar no mínimo 700 (setecentos) Mbps de throughput de Inspeção SSL; Suporte a, no mínimo, 1.400.000 (um milhão quatrocentos mil) conexões simultâneas; Suporte a, no mínimo, 42.000 (quarenta e duas mil) novas conexões por segundo; Possuir ao menos 5 (cinco) interfaces de 1GbE RJ45, sendo pelo menos 1 dela utilizada para gerenciamento; Possuir pelo menos 2 (duas) interfaces 1GbE SFP e seus módulos. Deverão ser fornecidos com 2 (dois) transceivers; Possuir pelo menos 1 (uma) interface do tipo console Suporte a, no mínimo, 15 (quinze) zonas de segurança; Possuir armazenamento de no mínimo 120 (cento e vinte) GB SSD; Fonte de alimentação interna ou externa, que opere com ajuste automático de tensão 110-220 Volts; Deve suportar a instalação em rack padrão 19” ou ser entregue com bandeja para a instalação em rack padrão 19”;	
	Especificação Técnica - GRUPO 2	
	SOLUÇÃO DE ANTIVÍRUS – LICENÇA PERPÉTUA	
	Características gerais antivírus para estações de trabalho e servidores: Entende-se por agente ou antivírus como sendo a ferramenta de proteção contra malwares ou vírus, termo a ser usado tanto para os componentes de proteção de estações de trabalho ou equipamentos servidores; A Solução deverá ser baseada na arquitetura cliente/servidor, sendo composta por componente de gerência centralizada e agentes antivírus: O serviço de gerência centralizada deverá ser onpremise, essa deverá ser disponibilizada por meio de appliance virtual do mesmo fabricante da solução ofertada ou a Contratada deverá realizar a instalação e configuração do(s) servidor(es) no ambiente disponibilizado, sem custo adicional para o Contratante;	

	O tráfego de dados entre os agentes e gerência centralizada deverá ocorrer através de conexão segura; Os componentes da solução deverão manter compatibilidade com o ambiente tecnológico da SSPDF; A solução deverá permitir instalação dos agentes de forma remota, por meio de GPO do Windows abrangendo todas as Seções e Subseções; A solução deverá ser fornecida pronta para utilização imediata, não sendo permitida apresentação de qualquer procedimento que configure o desenvolvimento da solução após a contratação; A solução deverá ser de um único fabricante, não devendo ser composta por módulos, softwares, scripts ou plug-ins de terceiros; Ressalvados os casos em que a solução ofertada utilize módulos do próprio Sistema Operacional, como Firewall e recursos de proteção antimalware nativos; A solução deverá oferecer proteção em camadas para detecção de malwares; O fabricante deverá oferecer serviço de análise e criação de solução específica para quando for identificado um possível malware não detectado pela solução antivírus; Entende-se por licença perpétua aquela que após o encerramento do contrato de suporte firmado pela administração publica, permanecerá funcionando, até que o fabricante informe que as licenças não receberão suporte e atualização, permanecendo com as antigas atualizações.	
	Gerenciamento centralizado: A console de gerência centralizada deverá oferecer interface baseada em modo gráfico (GUI) acessível por software ou navegador web de forma segura (HTTPS); Permitir o gerenciamento, controle, configuração e operação de todo parque (produtos instalados nos clientes e quaisquer outros módulos que componham a solução) de forma remota e centralizada; A gerência centralizada deverá estar em consonância e compatibilidade com o ambiente tecnológico exposto no item 04 deste Anexo; Deverá permitir acessos simultâneos de vários usuários à console da gerência (sessões); Deverá possuir uma base de dados centralizada para armazenamento das informações e logs dos clientes e da gerência; Deverá permitir a criação e distribuição de políticas e tarefas remotamente para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência; Deverá permitir operações de instalação, desinstalação e atualização dos módulos da solução para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência ou de GPO do Windows; Oferecer mecanismo de comunicação (via push) entre o(s) servidor(es) e os clientes para entrega de dados e informações; Oferecer mecanismo de comunicação (via pull) entre os clientes e o(s) servidor(es) para consulta de dados e informações; A instalação ou atualização dos módulos componentes da solução, distribuição de configurações, políticas e tarefas da gerência aos clientes deve ser realizada de forma silenciosa e sem necessidade de reinicialização ou logoff do equipamento e sem necessidades de aguardar alguma ação do usuário do equipamento; Deverá oferecer funcionalidade de execução, criação e customização de consultas às informações contidas na base de dados; Deverá possibilitar a disponibilização das informações em modo de gráficos ou tabelas; Deverá ser possível exportar as informações obtidas nas consultas em pelo menos um desses formatos: PDF, HTML, TXT, CSV ou Json; Deverá permitir criação de alertas e notificação de eventos para administradores e usuários determinados; Deverá possibilitar pesquisa no histórico de eventos; Deverá permitir execução de consultas por agendamento e envio do resultado via email; Deverá disponibilizar as seguintes consultas pré-definidas: Máquinas com maior número de ocorrência de vírus e ameaças; Usuários com maior número de ocorrência de vírus e ameaças; Histórico de infecções nas últimas 24 horas, 7 dias e 30 dias; Vírus e ameaças com maior número de registros nas últimas 24 horas, 7 dias e 30 dias; Versões dos produtos instalados; Versões das vacinas, quando for o caso, ou outras políticas de proteção adotadas. Deverá permitir criação de dashboards; Deverá permitir integração com o Active Directory da SSPDF para descoberta de equipamentos ou de forma nativa na própria solução; Deverá dar suporte a estrutura de florestas/domínios e subdomínios do Active Directory, refletindo a estrutura hierárquica da SSPDF no Active Directory: Deverá ser capaz de distinguir e agrupar equipamentos servidores, estações de trabalho e notebooks, de forma a definir agrupamentos distintos para aplicação de regras, tarefas e políticas; Deverá permitir que se configure diferentes políticas e tarefas para diferentes agrupamentos de computadores, seja para pontos específicos na estrutura em árvore (Seção, Subseção) como para demais grupos específicos (servidores ou estações de trabalho); Deverá possibilitar função de herança de políticas e tarefas entre os grupos e subgrupos, com possibilidade de quebra de herança; O acesso à console da gerência centralizada deverá ser efetuado mediante autenticação segura através de usuário cadastrado na base de dados da solução ou através de autenticação integrada com usuários do Active Directory; Todas as ações realizadas pelos usuários da gerência deverão ser registradas em log de auditoria, com no mínimo descrição da ação, nome do usuário, data e hora da ação realizada: Deve permitir cadastro de usuários com, pelo menos, os seguintes perfis (ou equivalentes): Administradores, com acesso a todas as funcionalidades da gerência e em toda a estrutura hierárquica da SSPDF; Administradores locais, com acesso a funcionalidades específicas e em pontos de domínios específicos da estrutura hierárquica da SSPDF; Visualização ou monitoramento, podendo abranger todo contexto da estrutura hierárquica da SSPDF ou pontos específicos; Deverá permitir instalação e desinstalação remota dos agentes antivírus, através da console de gerenciamento ou de GPO do Windows; A solução deverá ser capaz de detectar e listar equipamentos conectados na rede e que não possuam a solução instalada; Deverá identificar através da integração com o Active Directory, ou de forma nativa pela própria solução, computadores sem o agente antivírus instalado; Deverá apresentar a funcionalidade de instalação da solução nos equipamentos detectados através da listagem de equipamentos sem o antivírus instalado ou por meio do Active Directory ou por orquestradores. Deverá possibilitar o download de pacotes executáveis de instalação para proceder com instalação manual nos equipamentos, observado os sistemas operacionais suportados; Deverá permitir limpeza automática de agentes inativos por determinado período de tempo, liberando as respectivas licenças; Deverá ser possível criação de políticas para distribuição de atualizações para o parque gerenciado com periodicidade mínima diária; Deverá ser possível criação de políticas para distribuição de atualizações e vacinas para o parque gerenciado com periodicidade mínima diária; Deverá permitir configuração alternativa para permitir que o agente busque atualização na nuvem do fabricante quando estiver fora do escopo da gerência centralizada; As atualizações deverão ser do tipo incremental; Deverá permitir distribuição de versões diferentes da solução para diferentes grupos de equipamentos; Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, restaurar e excluir; Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, limpar e excluir; Deverá possibilitar restauração manual de arquivos quarentenados; Deverá permitir criar listas de exclusões ou exceções para determinados aplicativos ou diretórios e subdiretórios; Deverá utilizar os recursos locais de forma otimizada, sem impacto no desempenho do endpoint, ou possibilitar a configuração de baixo uso de recurso do dispositivo nas operações do agente antivírus; Deverá permitir criação de políticas para bloqueio de dispositivos de armazenamento externos; Deverá possibilitar extração de informações sobre dispositivos bloqueados, contendo no mínimo data e hora do ocorrido, equipamento onde o bloqueio ocorreu, rótulo do dispositivo bloqueado e usuário do sistema operacional logado durante o bloqueio; Deverá fornecer solução Sandbox, on-premise, para análise de malwares e mecanismo de reputação de softwares. Em caso de fornecimento do Sandbox on-premise a Contratada deverá instalar e fornecer todos os recursos logísticos e de infraestrutura necessários para implantação do equipamento no ambiente do Contratante, a exemplo de alimentação elétrica, cabeamento, sem custo adicional. As funcionalidades do serviço de Sandbox deverão ser integrados na gerência centralizada; Deverá possibilitar aplicar bloqueios e respostas para ameaças detectadas e analisadas pelo serviço de Sandbox em todo o parque; Deverá apresentar interface para investigação usando funcionalidades de Detecção e Resposta, sendo possível tomar ações para os equipamentos em análise;	
	Serviço de Desinstalação A desinstalação do parque atual existente na SSPDF deverá ser efetuada pela CONTRATADA;A CONTRATANTE deverá fornecer as credenciais necessárias para a execução da desinstalação, como usuário com privilégio. A estratégia a ser adotada na execução da desinstalação será previamente acordada entre o CONTRATANTE e a CONTRATADA. A desinstalação da ferramenta existente deverá ocorrer de forma silenciosa para o usuário; Em casos específicos onde seja necessário reboot, deverá ser informado para a CONTRANTE para que se monte uma estratégia de forma a não interromper o fluxo de trabalho onde se necessitar; O equipamento onde for instalado a nova solução deverá estar LIMPA e sem vestígios da instalação anterior, de forma que não se acarrete crashes e erros na instalação do novo agente e que não ocorra situações em que mais de 1 solução além da vigente por este certame estejam instaladas no equipamento ao mesmo tempo; Problemas na execução da desinstalação do agente deverão ser imediatamente comunicadas a CONTRATANTE;	
	Serviço de instalação e configuração A instalação deverá ocorrer em todo o âmbito da SSPDF; A instalação do agente deverá pressupor desinstalação da solução anterior; A instalação do agente deverá ser imperceptível para o usuário, de forma a não aparecer pop-ups, mensagens, caixas de diálogos solicitando ação de usuário e nem janelas modais, de forma a interromper de qualquer forma o usuário; Os serviços de instalação devem compreender a configuração da gerência centralizada em servidores virtuais para os componentes da solução on-premise, incluindo appliance virtual da gerência centralizada, banco de dados da solução e demais componentes a serem utilizados pela solução de gerência; Deverá possibilitar a instalação dos componentes da solução de forma a refletir a estrutura hierárquica da SSPDF, A instalação dos agentes deverá ser realizada de forma remota, abrangendo todas as Seções e Subseções; Deve permitir que se instale os agentes individualmente por computador ou em lote, para vários computadores; A interoperabilidade entre os componentes da solução deverá ser configurada por políticas na gerência e utilizando protocolos seguros; Deverá permitir que se programe através de políticas o agendamento da distribuição dos itens atualizados na gerência centralizada para os repositórios; Ao final do processo de instalação a CONTRATADA deverá fornecer os seguintes relatórios: Relação de todos os computadores contendo antivírus instalado, com no mínimo as seguintes informações, agrupados por localidade Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subsecretaria/SSPDF, contendo no mínimo: Versão de cada módulo da solução instalado; Versão da DAT, catálogo ou relatório de vacinas instaladas no endpoint; Versão de demais bibliotecas ou catálogos que compõem a solução instalado; Os relatórios serão utilizados para avaliar conformidade da prestação do serviço de instalação; Serão comparados com o quantitativo de máquinas ativas na SSPDF, utilizando a seguinte fórmula para apurar o índice de instalação: IND – Índice de instalação; QAI – Quantidade de computadores com antivírus instalado; QLA – Quantidade licenças adquiridas; Será dado aceite da solução quando o resultado da instalação IND possua valor igual ou superior a 0.8 – IND >= 0.8;	
	Garantia e atualização das licenças; A garantia técnica deverá ser contratada junto ao fabricante da solução, e sua vigência não poderá ser inferior ao período de 36(trinta e seis) meses, contados a partir da aceitação definitiva da solução; O atendimento do serviço de suporte técnico da garantia, deverá ser feito por intermédio da CONTRATADA ou diretamente com a fabricante através de portal específico para fins de suporte ou por e-mail; A garantia técnica deverá ser acionada nas situações específicas onde a CONTRATADA não conseguir solução para o problema ou quando o problema for detectado em relação aos elementos da solução contratada, tais como bugs ou algum mal funcionamento; A garantia técnica deverá incluir o fornecimento das atualizações do fabricante para a solução; As atualizações deverão ser fornecidas independente de solicitação da CONTRATANTE.	

Deverão ser providas atualizações das listas de definições de vírus e demais insumos para funcionamento atualizado da solução, de acordo com o mercado;
Deverá permitir atualizações da engine do agente (software), assim como da base de dados, padrões de comportamento e quaisquer outros elementos pertinentes à solução;
A garantia técnica contempla suporte técnico do fabricante, serviços de manutenções e atualizações da solução antivírus, base de dados de vacinas, bem como disponibilização de:
Solução de problemas que afetem elementos da solução, incluindo os softwares, atualizações e instalação, evoluções, patches, correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades, novos módulos, adequações e esclarecimento de dúvidas;
Manuais dos produtos e serviços ofertados, base de conhecimento para soluções conhecidas, canal de comunicação, esclarecimento de dúvidas e quaisquer outras informações solicitadas pela CONTRATANTE:
As informações prestadas deverão ser disponibilizadas preferencialmente no idioma Português do Brasil ou na falta deste, obrigatoriamente no idioma em Inglês;
Novas versões da solução lançadas pelo fabricante e lançamento de novos softwares em substituição da solução contratada, em caso de descontinuação do software fornecido.
Os serviços descritos neste item deverão ser prestados mediante abertura de chamado pela CONTRATANTE ou pela CONTRATADA, diretamente no portal de comunicação e suporte do fabricante, realizado por meio de e-mail e site de helpdesk;
A garantia deve incluir o funcionamento do serviço de sandbox e de detecção e resposta durante todo o período de vigência da garantia.

Solução de antivírus para estações de trabalho
Deverá ser compatível com as seguintes tecnologias de sistema operacional, no mínimo:
Windows 10;
Windows 11;
Deverá proporcionar proteção contra ameaças, tais como vírus, ransomwares, trojans, spywares, worms, keylogers, dentre outros malwares;
A solução e todos os seus componentes deverão funcionar como um agente composto por um executável que será instalado na estação de trabalho, podendo encapsular os diversos módulos que compõe a solução;
Caso a solução utilize de recursos de segurança nativos do Sistema Operacional, os mesmos serão considerados como módulos do agente único utilizado;
O módulo EDR poderá ser disponibilizado através de um executável ou módulo separado ao da solução de antivírus;
Deverá ser capaz de reconhecer ataques e ações maliciosas por assinatura, por análise heurística ou por machine learning;
Soluções que usem somente método de detecção por assinatura não serão aceitas;
Deverá possuir mecanismo de análise comportamental;
Deverá ser capaz de proteger ataques provenientes de malwares;
Deverá ser capaz de realizar proteção contra ameaças mesmo estando o dispositivo não conectado à internet;
Quando o equipamento estiver fora da cobertura da gerência centralizada deverá ser capaz de buscar atualizações na internet, na nuvem do fabricante;
Deverá permitir criar bloqueios personalizados, baseado no nome do aplicativo, caminho do aplicativo e hash do arquivo;
Deverá ser capaz de detectar, alertar e prevenir quando for detectado alguma ameaça;
Deverá ser capaz de prover proteção contra-ataques que explorem vulnerabilidades do sistema operacional do host, de acordo com o estabelecido no item 2.18.1 deste Anexo;
Deverá possuir proteção contra BOTs e variantes;
Deverá efetuar proteção permanente e em tempo real dos processos em memória;
Processos suspeitos deverão ser bloqueados;
Deverá possuir mecanismos de análise avançada para proteção e remediação de vírus de código polimorfos, ofuscados, criptografados e contra ameaças avançadas e persistentes, que não são detectadas pelos métodos convencionais de antivírus;
Deverá ser capaz de detectar variações de malwares geradas em memória principal;
Deverá oferecer tecnologia de proteção baseada em técnicas de Inteligência Artificial do tipo Machine Learning;
Em casos de aplicações com comportamento malicioso detectado, deverá efetuar bloqueios de processos e efetuar isolamento de comunicação;
Deverá oferecer proteção contra-ataques de 0Day (dia zero);
Deverá oferecer proteção contra Ransomwares, com capacidade de avaliar processos criptográficos em execução no sistema, exclusão de backups, número alto de operações de I/O no sistema de arquivos;
Deverá informar o nome ou endereço IP da origem do ataque ou infecção;
Deverá oferecer funcionalidade de controle de aplicações, identificando aplicações no mínimo pelo código Hash do executável, caminho e nome do aplicativo malicioso;
Deverá oferecer proteção contra vírus de macro e por scripts variados, incluindo bash e powershell;
Deverá oferecer mecanismo de bloqueio baseado em análise realizada pela central de inteligência do fabricante oriundo da nuvem;
Deverá implementar técnicas de Detecção e Resposta (EDR) para prover detecção e investigação para atividades suspeitas;
Deverá possibilitar visualizar toda a cadeia de ataque, inclusive os processos e aplicativos executados, arquivos e registros utilizados, endereços acessados, dentre outros;
Deverá oferecer proteção para alterações suspeitas de registro;
Deverá prover mecanismos para criação proteções personalizadas para detecção;
Deverá oferecer proteção contra processos que tentem alterar ou manipular indevidamente os componentes instalados e em execução do antivírus (autoproteção);
Deverá oferecer proteção contra-ataques direcionados;
Deverá gerar log local assim como enviá-los para a gerência;
Deverá permitir inclusão de exceções aplicações e caminhos;
A solução deverá oferecer proteção para ameaças em execução:
Na memória principal (RAM);
Em arquivos;
No tráfego de rede;
Em dados provenientes de browsers de navegação web (downloads, scripts, etc);
Em arquivos compactados (formatos zip, exe, cab, rar, etc);
Em processos de inicialização automática;
Em serviços criados/modificados;
Solução deverá efetuar a proteção permanente, em tempo real, quando arquivos forem acessados, lidos, gravados, alterados ou renomeados;
Deverá permitir bloqueio de alterações nas configurações do antivírus por parte do usuário, sendo permitido apenas por alterações de políticas ou mediante inserção de senha/password, definidos na gerência;
Deverá possibilitar a criação de lista de aplicações confiáveis (lista de exceções), a partir da gerência centralizada, para eliminação de detecções do tipo falso positivo;
Deverá oferecer a possibilidade de editar esta lista, com inclusão e remoção de aplicativos;
Deverá possuir a capacidade de detectar antivírus de outros fabricantes que possam acarretar incompatibilidade;
Deverá impedir execução e instalação de aplicativos cujo comportamento seja suspeito ou que constem na lista de aplicativos inseridos na gerência centralizada;
Deverá detectar e proteger em tempo real o computador contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de páginas da web e scripts em linguagens tais como javascript, vbscript, activex, etc;
Deverá oferecer mecanismo de controle de dispositivos externos;
A administração das regras da funcionalidade para controle mecanismos externos deverá ser realizada a partir da gerência centralizada;
O mecanismo de controle de dispositivos externos deverá possibilitar monitorar e bloquear dispositivos a partir de regras e políticas estabelecidas na gerencia centralizada, para no mínimo:
Dispositivos de rede externos (wifi portátil, dispositivos de dados móveis);
Transferências de dados para dispositivos mobile.;
Transferências de dados para dispositivos de armazenamento externos;
Possibilitar ações de bloqueio na execução de arquivos em transferência através de browsers e clientes de e-mail.
Deve oferecer ou executar uma das seguintes opções de ações corretivas para programas maliciosos detectados: bloquear o objeto, executar a limpeza da ameaça e executar ação de quarentena;
Os mecanismos de proteção deverão ser executados sem comprometer o desempenho dos computadores, de forma que não seja perceptível aos seus usuários e nem influenciem negativamente no rendimento de aplicações em servidores;
No mínimo as seguintes ocorrências deverão ser registradas em arquivo de log local ou enviadas para a gerência centralizada:
Atualização de engine e/ou repositório de vacinas.
Recebimento de políticas e tarefas da gerência;
Inicialização e finalização de varreduras, agendadas ou manuais, ou quando realizada por meio de análise dos processos em tempo real baseado em machine learning;
Detecção de alguma ameaça, registrando no mínimo as seguintes informações:
Nome da ameaça;
Tipo da ameaça;
Arquivo ou local infectado;
Data e hora da detecção;
Mecanismo que gerou a detecção;
Nome da máquina/endereço IP;
Ação realizada;
Usuário logado no sistema;
Deverá buscar por itens de atualização nos repositórios, configurado pela gerência, de acordo com topologia e políticas especificadas;
Deverá possibilitar mais de uma versão da ferramenta e seus insumos, para que em casos de incompatibilidades decorrentes de atualizações, seja possível reinstalar versões anteriores estáveis ou instalar versões novas em grupos específicos, para fins de testes de compatibilidade antes de instalação em todo parque;
Deverá fornecer informações do status do agente e de seus componentes, através da gerência com informações atualizadas com delay máximo de 5 minutos;
Deve ser disponibilizado nos idiomas português, preferencialmente, ou inglês;

Solução de antivírus para equipamentos servidores
Deverá ser compatível com as seguintes tecnologias de sistema operacional, no mínimo:
Windows Server 2008 R2;
Windows Server 2012;
Windows Server 2016;
Windows Server 2019 e posteriores;
VMware ESXi;
Deverá proporcionar proteção contra ameaças, tais como vírus, ransomwares, trojans, spywares, worms, keylogers, dentre outros malwares;
A solução e todos os seus componentes deverão funcionar como um agente composto por um executável único que será instalado na estação de trabalho, podendo encapsular os diversos módulos que compõe a solução;
Caso a solução utilize de recursos de segurança nativos do Sistema Operacional, os mesmos serão considerados como módulos do agente único utilizado;
Deverá ser capaz de reconhecer ataques e ações maliciosas por assinatura, por análise heurística ou por machine learning.
Soluções que usem somente método de detecção por assinatura não serão aceitas;
Deverá possuir mecanismo de análise comportamental;
Deverá ser capaz de proteger ataques provenientes de malwares;
Deverá ser capaz de realizar proteção contra ameaças mesmo estando o dispositivo não conectado à internet;
Deverá permitir criar bloqueios personalizados, baseado no nome do aplicativo, caminho do aplicativo e hash do arquivo;
Deverá ser capaz de detectar, alertar e prevenir quando for detectado alguma ameaça;
Deverá ser capaz de prover proteção contra ataques que explorem vulnerabilidades do sistema operacional do host, de acordo com o estabelecido no item 2.18.1 deste Anexo;
Deverá possuir proteção contra BOTs e variantes;
Deverá efetuar proteção permanente e em tempo real dos processos em memória;
Processos suspeitos deverão ser bloqueados;
Deverá possuir mecanismos de análise avançada para proteção e remediação de vírus de código polimorfos, ofuscados, criptografados e contra ameaças avançadas e persistentes, que não são detectadas pelos métodos convencionais de antivírus;
Deverá ser capaz de detectar variações de malwares geradas em memória principal;

Deverá oferecer tecnologia de proteção baseada em técnicas de Inteligência Artificial do tipo Machine Learning;
Em casos de aplicações com comportamento malicioso detectado, deverá efetuar bloqueios de processos e efetuar isolamento de comunicação;
Deverá oferecer proteção contra ataques de 0Day (dia zero);
Deverá oferecer proteção contra Ransomwares, com capacidade de avaliar processos criptográficos em execução no sistema, exclusão de backups, número alto de operações de I/O no sistema de arquivos;
Deverá informar o nome ou endereço IP da origem do ataque ou infecção;
Deverá ter a capacidade de bloquear ataques direcionados a aplicações em execução no servidor através de funcionalidade de proteção contra vulnerabilidades conhecidas e catalogadas através de CVE ou catálogo próprio, tanto para o sistema operacional quanto para aplicações instaladas no servidor;
O mecanismo deverá proteger no mínimo os seguintes softwares de terceiros: Apache, Tomcat, JBoss, Microsft IIS, SQL Server, PostgreSQL, Banco de Dados Oracle, MySQL e variantes, Wordpress, Joomla, Adobe entre outros;
Em caso de ataque a solução deverá detectar comportamentos maliciosos da aplicação web;
Para sistemas operacionais windows a solução deverá gerenciar o seu Firewall ou possuir Firewall bidirecional com detecção e proteção contra intrusões e ataques.
Firewall deverá possibilitar ações como permitir e bloquear: portas, range de portas, IPs, range de IPs e redes;
Deverá ser possível aplicar regras de permitir todo tráfego ou bloquear todo tráfego;
Deverá oferecer funcionalidade de controle de aplicações, identificando aplicações no mínimo pelo código Hash do executável, caminho e nome do aplicativo malicioso;
Deverá oferecer proteção contra vírus de macro e por scripts variados, incluindo bash e powershell;
Deverá oferecer mecanismo de bloqueio baseado em análise realizada pela central de inteligência do fabricante oriundo na nuvem;
Deverá implementar técnicas de Detecção e Resposta (EDR) para prover detecção e investigação para atividades suspeitas
Deverá possibilitar visualizar toda a cadeia de ataque, inclusive os processos e aplicativos executados, arquivos e registros utilizados, endereços acessados, dentre outros;
Deverá oferecer proteção para alterações suspeitas de registro;
Deverá prover mecanismos para criação proteções personalizadas para detecção;
Deverá oferecer proteção contra processos que tentem alterar ou manipular indevidamente os componentes instalados e em execução do antivírus (autoproteção);
Deverá oferecer proteção contra ataques direcionados;
Deverá gerar log local assim como envia-los para a gerência, ou enviar logs em tempo real para a gerência centralizada;
Deverá permitir inclusão de exceções aplicações e caminhos;
A solução deverá oferecer proteção para ameaças em execução:
Na memória principal (RAM);
Em arquivos;
No tráfego de rede;
Em dados provenientes de browsers de navegação web (downloads, scripts, etc);
Em arquivos compactados (formatos zip, exe, cab, rar, etc);
Em processos de inicialização automática;
Em serviços criados/modificados;
Solução deverá efetuar a proteção permanente, em tempo real, quando arquivos forem acessados, lidos, gravados, alterados ou renomeados;
Deverá possibilitar a criação de lista de aplicações confiáveis (lista de exceções), a partir da gerencia centralizada, para eliminação de detecções do tipo falso positivo;
Deverá oferecer a possibilidade de editar esta lista, com inclusão e remoção de aplicativos;
Deverá possuir a capacidade de detectar antivírus de outros fabricantes que possam acarretar em incompatibilidade;
Deverá impedir execução e instalação de aplicativos cujo comportamento seja suspeito ou que constem na lista de aplicativos inseridos na gerência centralizada;
Deverá detectar e proteger em tempo real o computador contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de páginas da web e scripts em linguagens tais como javascript, vbscript, activex, etc;
Deve oferecer ou executar uma das seguintes opções de ações corretivas para programas maliciosos detectados: bloquear o objeto, executar a limpeza da ameaça e executar ação de quarentena;
Os mecanismos de proteção deverão ser executados sem comprometer o desempenho dos computadores, de forma a não influenciar negativamente no rendimento de aplicações em servidores;
No mínimo as seguintes ocorrências deverão ser registradas em arquivo de log local ou enviadas para a gerência centralizada:
Atualização de engine e/ou repositório de vacinas.
Recebimento de políticas e tarefas da gerência;
Inicialização e finalização de varreduras, agendadas ou manuais, ou quando realizada por meio de análise dos processos em tempo real baseado em machine learning;
Detecção de alguma ameaça, registrando no mínimo as seguintes informações:
Nome da ameaça;
Tipo da ameaça;
Arquivo ou local infectado;
Data e hora da detecção;
Mecanismo que gerou a detecção (varredura agendada, manual, em tempo real);
Nome da máquina/endereço IP;
Ação realizada;
Usuário logado no sistema;
Deverá buscar por itens de atualização nos repositórios,configurado pela gerência, de acordo com topologia e políticas especificadas;
Deverá possibilitar mais de uma versão da ferramenta e seus insumos, para que em casos de incompatibilidades decorrentes de atualizações, seja possível reinstalar versões anteriores estáveis ou instalar versões novas em grupos específicos, para fins de testes de compatibilidade antes de instalação em todo parque;
Deverá fornecer informações do status do agente e de seus componentes, através da gerência com informações atualizadas com delay máximo de 5 minutos;
Deve ser disponibilizado nos idiomas: português (preferencialmente) ou inglês;

ANEXO IV - ORDEM DE SERVIÇO

OS Nº	Data Emissão	Nº do Contrato	Data de Assinatura do Contrato
xx/xxxx	**xx/xx/xxxx**	**xx/xxxx**	**xx/xx/xxxx**

Bloco 1 – INFORMAÇÕES DO FORNECEDOR	
Razão Social: XXXXXXX	
Endereço: XXXXX - BRASÍLIA/DF	**Telefone: (061) XXXX-XXXX**
CNPJ/MF: XX.XXX.XXX/0001-XX	

Bloco 2 – INFORMAÇÕES DO EXECUTOR	
Nome: XXXXX	
CNPJ/MF: XX.XXX.XXX/0001-XX	

Bloco 3 – ESPECIFICAÇÃO DE BENS E PRODUTOS			
1. Descrição: **Escrever o objeto declarado em contrato.**			
2. Período de Entrega			
3. Especificação			
Descrição do Produto	**Qtde.**	**Valor Unitário**	**Valor Total**
4. Local de Realização			

Bloco 4 – ESPECIFICAÇÕES TÉCNICAS PARA REALIZAÇÃO DOS SERVIÇOS
Termo de Concordância
Declaramos nossa concordância em executar as atividades descritas nesta OS, de acordo com as especificações técnicas estabelecidas em contrato com a Secretaria de Segurança Pública do Distrito Federal - SSPDF.
Brasília-DF, xx de _____ de xxxx. _____ _____

Bloco 5 – ACEITAÇÃO PELO FORNECEDOR
Termo de Concordância
Declaramos nossa concordância em executar as atividades descritas nesta OS, de acordo com as especificações técnicas estabelecidas em contrato com a Secretaria de Segurança Pública do Distrito Federal - SSPDF.
Brasília-DF, xx de _____ de xxxx. _____ _____

Bloco 6 – AUTORIZAÇÃO FINAL
Autorização
Autorizamos a execução da presente Ordem de Serviço de acordo com as especificações nela contidas bem como pela sua conformidade com o contrato assinado.
Brasília-DF, xx de _____ de xxxx. _____ _____ _____ XXXXXXXX XXXXXXXXX

Requisitante	Executor do Contrato

ANEXO V - RELATÓRIO DE VISITA TÉCNICA

1. IDENTIFICAÇÃO DA CONTRATADA

NOME:	**CNPJ:**
ENDEREÇO:	
Técnico Responsável: **CPF:**	

2. ESPECIFICAÇÕES DOS SERVIÇOS

Descrição		
Nº do chamado/protocolo: ___/_____	Data de abertura: [__/__/____]	Contrato n. /201X Hora de abertura do chamado: [__:__:__] Hora do Início do Atendimento: [__:__:__] Hora do término do Atendimento: [__:__:__]

3. ATIVIDADES EXECUTADAS:

Identificação do(s) equipamento(s) avaliados:
Atividades desenvolvidas: ***Demanda: Atividades:*** ***Defeitos detectados:*** ***Solução apresentada:***

4. DE ACORDO:

Data	**Responsável da CONTRATADA**	**Assinatura**

5. APROVAÇÃO

Data	**Responsável da CONTRATADA**	**Assinatura**
Ressalvas ou observações:		

Notas: a) O Modelo aqui apresentado é ilustrativo e poderá sofrer ajustes, se for o caso, na implantação do processo operacional junto à CONTRATADA.

ANEXO VI - DECLARAÇÃO DE DESISTÊNCIA DE VISTORIA

Declaro que a empresa _____, CNPJ Nº:_____, sediada à _____, telefone _____, não teve interesse em realizar a vistoria nas instalações d para verificação e conhecimento de todas as condições físicas, padrões e complexidade do(s) local(is) onde será prestado o serviço, responsabilizando inteiramente pela prestação do serviço e plena ciência das condições estabelecidas no instrum Pregão nº _____/_____.

Brasília - DF, _____ de _____ de _____.

Assinatura/Carimbo do Declarante

Assinatura/Carimbo da Empresa

ANEXO VII - TERMO DE SIGILO E CONFIDENCIALIDADE

INTRODUÇÃO

A **<PESSOA JURÍDICA>**, 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 CONTR **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 **SECRETA PÚBLICA DO DISTRITO FEDERAL**, doravante referida simplesmente como **SSPDF**, 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 SSPDF, tem acesso a informações que pertencem à SSPDF, 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, projet 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 contra

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 SSPDF, referido n diferentemente. Em hipótese alguma, a ausência de manifestação expressa da SSPDF 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

Subcláusula Segunda - A CONTRATADA obriga-se a informar imediatamente à SSPDF qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, 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 alg 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 presta 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 SSPDF, 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 co 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 CONFIDENCIALIDADE, a que teve acesso em d contratual com a SSPDF.

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 SSPDF.

Por estar de acordo, a CONTRATADA, por meio de seu representante, firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em 2 (duas) vias de igual teor e forma.

Brasília-DF, _

_____

Servidor Designado pela SSP/DF

_____

Representante Legal da Empresa

ANEXO VIII - TERMO DE CIÊNCIA

INTRODUÇÃO

O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na SSP/DF. No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Executor do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados.

1. IDENTIFICAÇÃO

Contrato nº:

Objeto:

Contratada:

CNPJ:

Preposto:

Executor do Contrato:

Matrícula do executor do contrato:

2. CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	**Matrícula**	**Assinatura**
...	...	...

Brasília-DF, ____de _____ de 20___.

Documento assinado eletronicamente por **HELIO DE FARIAS SOARES - Matr.1713991-0**, **Coordenador(a) de Infraestrutura**, em 08/12/2023, às 10:00, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **GLAUCIO SILVEIRA E SILVA - Matr.1691710-3**, **Assessor(a) Técnico(a).**, em 08/12/2023, às 10:01, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **DOUGLAS WILLIAN BARBOSA MOREIRA - Matr.1699997-5**, **Diretor(a) de Suporte**, em 08/12/2023, às 10:40, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **MAXWELL AMÉRICO MARINELLO - Matr.0176457-8**, **Assessor(a) Técnico(a).**, em 08/12/2023, às 10:46, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **FÁBIO MARTINS DA SILVA - Matr.1712453-0**, **Subsecretário(a) de Modernização Tecnológica**, em 08/12/2023, às 11:15, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **122736659** código CRC= **9DF39FAB**.

ANEXO II AO EDITAL – DECLARAÇÃO

(OBRIGATÓRIA PARA TODOS OS LICITANTES)

DECLARAÇÃO – ATENDIMENTO DA LEI DISTRITAL Nº 4.770/2012 (SUSTENTABILIDADE AMBIENTAL)

Ref.: PREGÃO Nº _____/20___ - SSPDF

A empresa _____, inscrita no CNPJ nº _____, por intermédio de seu representante legal o(a) Sr(a) _____, portador(a) da Carteira de Identidade nº _____ e do CPF nº _____, **DECLARA QUE ATENDE OS CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL** previstos no art. 7º da Lei Distrital nº 4.770/2012, **em especial que produz/comercializa bens**:

a) constituídos por material reciclado, atóxico e biodegradável, na forma das normas da Associação Brasileira de Normas Técnicas – ABNT;

b) que ofereçam menor impacto ambiental em relação aos seus similares;

c) que não contém substâncias perigosas acima dos padrões tecnicamente recomendados por organismos nacionais ou internacionais;

d) acondicionados em embalagem adequada, feita com a utilização de material reciclável, com o menor volume possível;

e) que funcionem com baixo consumo de energia ou de água;

f) que sejam potencialmente menos agressivos ao meio ambiente ou que, em sua produção, signifiquem economia no consumo de recursos naturais;

g) que possuam certificado emitido pelos órgãos ambientais;

h) que possuam certificação de procedência de produtos.

Brasília-DF, _____ de _____ de _____.

_____

Representante Legal

ANEXO III AO EDITAL

DECLARAÇÃO PARA OS FINS DO DECRETO N° 39.860, DE 30 DE MAIO DE 2019

(Portaria nº 356/2019-CGDF)

ÓRGÃO: Secretaria de Estado de Segurança Pública do Distrito Federal
PROCESSO:
MODALIDADE DE LICITAÇÃO: Pregão Eletrônico
NÚMERO DA LICITAÇÃO:
LICITANTE:
CNPJ:
INSCRIÇÃO ESTADUAL/DISTRITAL:
REPRESENTANTE LEGAL:
CPF:

A pessoa jurídica acima identificada, por intermédio de seu representante legal, declara que não incorre nas vedações previstas no art. 9º da Lei nº 8.666, de 21 de junho de 1993, e no art. 1º do Decreto nº 39.860, de 30 de maio de 2019. Essa declaração é a expressão da verdade, sob as penas da lei.

Brasília, _____ de _____ de _____

_____

Assinatura

ANEXO IV AO EDITAL – MINUTA DE CONTRATO

(AQUISIÇÃO COM PRAZO DE ENTREGA INTEGRAL)

Havendo irregularidades neste instrumento, entre em contato com a Ouvidora de Combate à Corrupção, no telefone 0800-6449060

CONTRATO DE AQUISIÇÃO DE BENS n.º __/____ - SSPDF, nos termos do Padrão nº 07/2002.

Processo n.º (LINK SEI).

CLÁUSULA PRIMEIRA – DAS PARTES

1.1. O Distrito Federal, por meio do **FUNDO DE SEGURANÇA PÚBLICA DO DISTRITO FEDERAL,** inscrito no **CNPJ sob o nº 33.158.099/0001-03**, representado neste instrumento pelo Secretário de Estado de Segurança Pública _____, portador do RG n.º _____ e do CPF n.º _____, com a delegação de competência prevista nas Normas de Planejamento, Orçamento, Finanças, Patrimônio e Contabilidade do Distrito Federal (Decreto nº 32.598, de 15/12/2010) e a empresa _____, doravante denominada **CONTRATADA**, inscrita no CNPJ sob o nº __.___.___/____-__, com sede na _____, CIDADE-UF, Tel.: (__) ____-____ e (__) ____-____, representado por _____, portador(a) do RG nº _____ SSP/__ e do CPF nº ___.___.___-__, na qualidade de _____.

CLÁUSULA SEGUNDA – DO PROCEDIMENTO

2.1. O presente Contrato obedece aos termos do Edital de Pregão Eletrônico nº ____ (LINK SEI), da Proposta (LINK SEI), da Lei nº 10.520/2002, pelo Decreto Federal nº 10.024/209, recepcionado no DF pelo Decreto distrital nº 40.205/2019, _____ e da Lei n.º 8.666/1993 e alterações subsequentes, além de outras normas aplicáveis à espécie.

ATENÇÃO! Verificar no processo quais as Leis/Decretos são aplicáveis e devem constar no corpo da cláusula segunda.

CLÁUSULA TERCEIRA – DO OBJETO

3.1. O Contrato tem por objeto a aquisição de solução de armazenamento de dados, para atender demanda da Secretaria de Estado de Segurança Pública do Distrito Federal (SSP/DF), consoante especifica o Edital de Pregão Eletrônico nº _____ (fls. _____) e da Proposta de fls. _____, que passam a integrar o presente Termo.

ATENÇÃO: INDICAR CLARAMENTE O OBJETO, COM SUAS PRINCIPAIS CARACTERÍSTICAS E A QUANTIDADE.

CLÁUSULA QUARTA – DA FORMA DE FORNECIMENTO

4.1. A entrega do objeto processar-se-á de forma **INTEGRAL** em **até 60 dias úteis,** a contar **da assinatura do contrato,** conforme especificação contida no Edital de Pregão Eletrônico nº ____/_____-SSP (fls. ____) e na Proposta de fls. _____, facultada sua prorrogação nas hipóteses previstas no § 1º do art. 57 da Lei nº 8.666/1993, devidamente justificada por escrito e previamente autorizada pela autoridade competente para celebrar o Contrato.

4.2. A entrega se dará nos Edifícios da sede da SSPDF e no CIOB, localizados no SAM, conjunto A, Asa Norte, Brasília/DF, telefone: (61) 3441-8820, em dia de expediente da SSPDF, em horário de 08h00 às 17h00.

CLÁUSULA QUINTA – DO VALOR

5.1. O valor total do Contrato é de R$ _____ (_____), devendo a importância ser atendida à conta de dotações orçamentárias consignadas no orçamento corrente – Lei Orçamentária _____.

5.2. Observado o interregno mínimo de um ano a partir da data limite para apresentação da proposta, o Contrato celebrado poderá, à pedido da empresa, ter seu valor anualmente reajustado, pelo Índice Nacional de Preços ao Consumidor Amplo - IPCA.

5.3. O prazo para a CONTRATADA requerer o reajuste contratual estipulado na Cláusula 5.2. extinguir-se-á:

5.3.1. com o fim do prazo de vigência, momento em que ocorrerá a preclusão temporal; ou

5.3.2. com a formalização após o interregno mínimo de um ano de Termo Aditivo de alteração quantitativa/qualitativa ou de revisão contratual, momento em que ocorrerá a preclusão consumativa.

5.4. Os efeitos financeiros decorrentes do reajuste contratual vigorarão a partir da data do pedido

CLÁUSULA SEXTA – DA DOTAÇÃO ORÇAMENTÁRIA

6.1. A despesa correrá à conta da seguinte Dotação Orçamentária:

I – Unidade Orçamentária: _____.

II – Programa de Trabalho: _____.

III – Natureza da Despesa: _____.

IV – Fonte de Recursos: _____.

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 feito, de acordo com as Normas de Execução Orçamentária, Financeira e Contábil do Distrito Federal, em parcela (s), mediante a apresentação de Nota Fiscal, liquidada até 30 (trinta) dias de sua apresentação, devidamente atestada pelo Executor do Contrato.

7.1.1. A Nota Fiscal apresentada para fins de pagamento deve ser emitida pelo mesmo CNPJ constante na proposta de preços, **à exceção de empresas que sejam matriz e filial** (Acórdão nº 3.056/2008 – TCU – Plenário);

7.1.2. As Notas Fiscais apresentadas com CNPJ divergente da proposta de preços, **à exceção de empresas matriz e filial** (item 7.1.1, *in fine*), serão devolvidas pela Administração, para a devida correção (emissão de Nota Fiscal com o CNPJ correto).

7.2. A Nota Fiscal deverá ser emitida em nome do **FUNDO DE SEGURANÇA PÚBLICA DO DISTRITO FEDERAL, CNPJ: 33.158.099/0001-03**.

7.3. Para efeito de pagamento, a Contratada deverá apresentar os seguintes documentos:

7.3.1. Prova de Regularidade junto à **Fazenda Nacional** (Débitos e Tributos Federais), à **Dívida Ativa da União** e junto à **Seguridade Social** (contribuições sociais previstas nas alíneas "a" a "d" do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991 – contribuições previdenciárias e as às de terceiros), fornecida por meio da Certidão Negativa, ou Positiva com Efeito de Negativa, de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União;

7.3.2. Certificado de Regularidade do Fundo de Garantia por Tempo de Serviço – FGTS, fornecido pela CEF – Caixa Econômica Federal, devidamente atualizado (Lei n.º 8.036/1990);

7.3.3. Certidão de Regularidade com a Fazenda do Distrito Federal;

7.3.4. Certidão de regularidade relativa a débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa, em plena validade, que poderá ser obtida no site www.tst.jus.br/certidao.

7.4. Os pagamentos, pela SSPDF, de valores iguais ou superiores a R$ 5.000,00 (cinco mil reais) serão feitos exclusivamente mediante crédito em conta corrente, em nome do beneficiário, junto ao Banco de Brasília S/A – BRB (Decreto Distrital nº 32.767, de 17 de fevereiro de 2011), exceto:

7.4.1. Os pagamentos às empresas vinculadas ou supervisionadas pela Administração Pública federal;

7.4.2. Os pagamentos efetuados à conta de recursos originados de acordos, convênios ou contratos que, em virtude de legislação própria, só possam ser movimentados em instituições bancárias indicadas nos respectivos documentos;

7.4.3. Os pagamentos a empresas de outros Estados da federação que não mantenham filiais e/ ou representações no DF e que venceram processo licitatório no âmbito deste ente federado.

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

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

CLÁUSULA OITAVA – DO PRAZO DE VIGÊNCIA

8.1. O contrato terá vigência de 48 (quarenta e oito) meses, a contar de sua assinatura.

CLÁUSULA NONA – DA GARANTIA CONTRATUAL

9.1. A garantia para a execução do Contrato será de 5% (cinco por cento) do valor do contrato, mediante uma das seguintes modalidades a escolha do Contratado: fiança bancária, seguro garantia ou caução em dinheiro ou em títulos da dívida pública, devendo os dois primeiros ser 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;

9.2. A garantia deverá ter validade igual ou superior a 90 dias após a vigência do contrato;

9.3. Toda e qualquer garantia prestada pela Licitante vencedora:

9.3.1. quando em dinheiro, somente poderá ser levantada 90 dias após a extinção do contrato, atualizada monetariamente;

9.3.2. poderá, a critério da SSPDF, ser utilizada para cobrir eventuais multas e/ou para cobrir o inadimplemento de obrigações contratuais, sem prejuízo da indenização eventualmente cabível. Nesta hipótese, no prazo máximo de 15 (quinze) dias corridos após o recebimento da notificação regularmente expedida, a garantia deverá ser reconstituída;

9.3.3. ficará retida no caso de rescisão contratual, até definitiva solução das pendências administrativas ou judiciais.

9.4. Caso a Contratada opte pela caução em dinheiro, a empresa deverá realizar TED ou depósito para a Secretaria de Estado de Fazenda do Distrito Federal, CNPJ 00.394.684/0001-53, no Banco Regional de Brasília (BRB) Agência 100; Conta 800482-8.

CLÁUSULA DÉCIMA – DA GARANTIA OU ASSISTÊNCIA TÉCNICA

10.1. A garantia ou assistência técnica do bem está especificada de acordo com o Termo de Referência e com a proposta, anexos a este Termo.

CLÁUSULA DÉCIMA PRIMEIRA – DA RESPONSABILIDADE DO DISTRITO FEDERAL

11.1. 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.

CLÁUSULA DÉCIMA SEGUNDA – DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

12.1. A Contratada fica obrigada a apresentar ao Distrito Federal, sem prejuízo do estabelecido no Termo de Referência:

12.1.1. até o quinto dia útil do mês subsequente, comprovante de recolhimento dos encargos previdenciários, resultantes da execução do Contrato;

12.1.2. comprovante de recolhimento dos encargos trabalhistas, fiscais e comerciais.

12.2. A Contratada deverá:

12.2.1. garantir a boa qualidade dos produtos fornecidos à Administração, bem como efetuar a sua substituição, às suas expensas, no prazo estipulado no Edital, após a comunicação da Administração, de qualquer produto entregue, que não esteja de acordo com as especificações ou em relação ao qual, posteriormente, não obstante os testes realizados, venha a se constatar qualquer adulteração ou vício;

12.2.2. zelar e garantir a boa qualidade dos produtos fornecidos à Administração, em consonância com os parâmetros de qualidade fixados e exigidos pelas normas técnicas pertinentes, expedidas pelo poder Público;

12.2.3. cumprir rigorosamente as normas técnicas relacionadas ao transporte dos produtos, responsabilizando-se pela qualidade das embalagens que acondicionam o produto;

12.2.4. responsabilizar-se pelo pagamento de taxas, fretes, seguros, transporte, embalagens e demais encargos decorrentes do fornecimento do objeto deste contrato;

12.2.5. responder por violações a direito de uso de materiais, métodos ou processos de execução protegidos por marcas ou patentes, arcando com indenizações, taxas e/ou comissões que forem devidas;

12.2.6. entregar os produtos observando que o acondicionamento e o transporte devem ser feitos dentro do preconizado para os produtos e devidamente protegido do pó e variações de temperatura. No caso de produtos termolábeis, a embalagem e os controles devem ser apropriados para garantir a integridade do produto, devendo ser utilizadas preferencialmente fitas especiais para monitoramento de temperatura durante o transporte;

12.2.7. entregar os produtos observando que as embalagens externas devem apresentar as condições corretas de armazenamento do produto (temperatura, umidade, empilhamento, etc.);

12.2.8. entregar os produtos observando que as embalagens primárias individuais dos produtos devem apresentar o número do lote, data de fabricação e prazo de validade.

12.3. Constitui obrigação da Contratada o pagamento dos salários e demais verbas decorrentes da prestação de serviço;

12.4. A Contratada responderá pelos danos causados por seus agentes;

12.5. A Contratada se obriga a 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;

12.6. Responsabilizar-se por quaisquer danos pessoais e/ ou materiais, causados por técnicos (empregados) e acidentes causados por terceiros, bem como pelo pagamento de salários, encargos sociais e trabalhistas, tributos e demais despesas eventuais, decorrentes da prestação dos serviços;

12.7. A Contratada declarará a inexistência de possibilidade de transferência ao Distrito Federal de responsabilidade por encargos trabalhistas, fiscais, comerciais e/ou previdenciários porventura inadimplidos, bem como a inexistência de formação de vínculo empregatício entre os empregados da Contratada e a Administração Pública.

CLÁUSULA DÉCIMA TERCEIRA – DA ALTERAÇÃO CONTRATUAL

13.1. Toda e qualquer alteração deverá ser processada mediante a celebração de Termo Aditivo, com amparo no art. 65 da Lei nº 8.666/1993, vedada a modificação do objeto.

13.2. A alteração de valor contratual, decorrente do reajuste de preço, 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 QUARTA – DAS PENALIDADES

14.1. Pelo descumprimento de quaisquer cláusulas ou condições do presente Contrato, serão aplicadas as penalidades estabelecidas no Decreto 26.851/2006 e alterações posteriores.

CLÁUSULA DÉCIMA QUINTA – DA RESCISÃO AMIGÁVEL

15.1. O Contrato poderá ser rescindido amigavelmente, por acordo entre as partes, reduzida a termo no processo, desde que haja conveniência para a Administração, bastando para tanto, manifestação escrita de uma das partes, com antecedência mínima de 60 (sessenta) dias, sem interrupção do curso normal da execução do Contrato, devendo ser precedida de autorização escrita e fundamentada da autoridade competente.

CLÁUSULA DÉCIMA SEXTA – DA RESCISÃO

16.1. 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 8.666/1993, sujeitando-se a Contratada às consequências determinadas pelo art. 80 desse diploma legal, sem prejuízo das demais sanções cabíveis.

CLÁUSULA DÉCIMA SÉTIMA – DOS DÉBITOS PARA COM A FAZENDA PÚBLICA

17.1. 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 OITAVA – DO EXECUTOR

18.1. A Secretaria de Estado de Segurança Pública do Distrito Federal designará um Executor para o Contrato, que desempenhará as atribuições previstas nas Normas de Execução Orçamentária, Financeira e Contábil do Distrito Federal.

CLÁUSULA DÉCIMA NONA – DA PUBLICAÇÃO E DO REGISTRO

19.1. 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. Os contratos e seus aditamentos serão lavrados na Coordenador de Planejamento, Licitações e Compras Diretas da SSPDF, a qual manterá arquivo cronológico dos seus autógrafos e registro sistemático do seu extrato, que se formalizam por instrumento lavrado em cartório de notas, de tudo juntando-se cópia ao processo que lhe deu origem, nos termos do art. 60, *caput*, da Lei 8.666/1993.

CLÁUSULA VIGÉSIMA – DO FORO

20.1. Fica eleito o foro de Brasília, Distrito Federal, para dirimir quaisquer dúvidas relativas ao cumprimento do presente Contrato.

Pelo Distrito Federal:	**Pela Contratada:**
_____	_____
Secretário de Estado de Segurança Pública	Representante legal

ANEXO V

REGULAMENTAÇÃO DAS PENALIDADES NO ÂMBITO DO DISTRITO FEDERAL

DECRETO DO DF 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 conferem o inciso VII, art. 100 da Lei Orgânica do Distrito Federal, e tendo em vista o disposto nos arts. 81, 86, 87 e 88 da Lei Federal nº 8.666, de 21 de junho de 1993, e no art. 7º da Lei Federal nº 10.520, de 17 de julho de 2002, bem como o disposto no art. 68 da Lei Federal nº 9.784, de 29 de janeiro de 1999, e ainda, a centralização de compras instituída nos termos da Lei Distrital nº 2.340, de 12 de abril de 1999, e as competências instituídas pela Lei Distrital nº 3.167, de 11 de julho de 2003, DECRETA:

CAPÍTULO I

DAS SANÇÕES ADMINISTRATIVAS

SEÇÃO I

Disposições Preliminares

Art. 1º A aplicação das sanções de natureza pecuniária e restritiva de direitos pelo não cumprimento das normas de licitação e/ou de contratos, em face do disposto nos arts. 81, 86, 87 e 88, da Lei Federal nº 8.666, de 21 de junho de 1993, e no art. 7º da Lei Federal nº 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 neste 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 nº 8.666, de 21 de junho de 1993, nos termos do disposto no § 1º do art. 2º da Lei Distrital nº 2.340, de 12 de abril de 1999.

SEÇÃO II

Das Espécies de Sanções Administrativas

Art. 2º As licitantes e/ou contratadas que não cumprirem integralmente as obrigações assumidas, garantida a prévia defesa, estão sujeitas às seguintes sanções:

I - advertência;

II - multa; e

III - suspensão temporária de participação em licitação, e impedimento de contratar com a Administração do Distrito Federal:

1. para a licitante e/ou contratada através da modalidade pregão presencial ou eletrônico que, convocada 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 a licitante e/ou contratada será descredenciada 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;

2. para as licitantes nas demais modalidades de licitação previstas na Lei nº 8.666, de 21 de junho 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 a contratada 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 a interessada, no respectivo processo, no prazo de 5 (cinco) dias úteis.

SUBSEÇÃO I

Da Advertência

Art. 3º A advertência é o aviso por escrito, emitido quando a licitante e/ou contratada 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; e

II - pelo ordenador de despesas do órgão contratante 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. 4º A multa é a sanção pecuniária que será imposta à contratada, pelo ordenador de despesas do órgão contratante, por 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;

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;

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; e

V - até 20% (vinte por cento) sobre o valor do contrato/nota de empenho, pelo descumprimento de qualquer cláusula do contrato, exceto prazo de entrega.

§ 1º A multa será formalizada por simples apostilamento contratual, na forma do art. 65, § 8º, da Lei nº 8.666, de 21 de junho de 1993 e será executada após regular processo administrativo, oferecido à contratada 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 21 de junho 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 à contratada; e

III - mediante procedimento administrativo ou judicial de execução.

§ 2º Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá à contratada pela sua diferença, devidamente atualizada pelo Índice Geral de Preços - Mercado (IGP-M) ou equivalente, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrados judicialmente.

§ 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; e

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 d*este artigo.

§ 7º A sanção pecuniária prevista no inciso IV do *cap*ut deste artigo não se aplica nas hipóteses de rescisão contratual que não ensejam penalidades.

Art. 4-A A multa de que trata o art. 4º deste Decreto será aplicada, nas contratações previstas na Lei Federal nº 12.232, de 29 de abril de 2010, 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;

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;

III - 1% (um por cento) do valor do contrato em caso de recusa injustificada do adjudicatário em assinar o termo contratual dentro do prazo estabelecido pela Administração;

IV - 1% (um por cento) sobre o valor do contrato que reste executar ou sobre o valor da dotação orçamentária que reste executar, o que for menor, em caso de rescisão contratual;

V - até 1% (um por cento) sobre o valor do contrato que reste executar ou sobre o valor da dotação orçamentária que reste executar, o que for menor, pelo descumprimento de qualquer cláusula do contrato, respeitado o disposto nos incisos I e II.

SUBSEÇÃO III

Da Suspensão

Art. 5º A suspensão é a sanção que impede temporariamente o fornecedor de participar de licitações e de contratar com a Administração, e, se aplicada em decorrência de licitação na modalidade pregão, ainda suspende o registro cadastral da licitante e/ou contratada no Cadastro de Fornecedores do Distrito Federal, instituído pelo Decreto nº 25.966, de 23 de junho de 2005, e 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 - SUCOM, ou pelo órgão integrante do Sistema de Registro de Preços, a licitante e/ou contratada permanecer inadimplente;

II - por até 90 (noventa) dias, em licitação realizada na modalidade pregão presencial ou eletrônico, 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; e

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; e

c) receber qualquer das multas previstas no artigo anterior e não efetuar o pagamento.

§ 1º 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; e

II - o ordenador de despesas do órgão contratante, 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.

§ 2º A penalidade de suspensão será publicada no Diário Oficial do Distrito Federal.

§ 3º 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. 6º A declaração de inidoneidade será aplicada pelo Secretário de Estado ou autoridade equivalente do órgão de origem, à vista dos motivos informados na instrução processual.

§ 1º 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 a contratada ressarcir a Administração pelos prejuízos resultantes de sua conduta e após decorrido o prazo da sanção.

§ 2º 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 21 de junho de 1993.

CAPÍTULO II

DAS DEMAIS PENALIDADES

Art. 7º 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 - SUCOM, 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.

Parágrafo único. Aplicam-se a este artigo as disposições dos §§ 2º e 3º do art. 5º deste Decreto.

Art. 8º 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 21 de junho de 1993 ou 10.520, de 17 de julho 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; e

III - demonstrarem não possuir idoneidade para contratar com a Administração, em virtude de atos ilícitos praticados.

CAPÍTULO III

DO DIREITO DE DEFESA

Art. 9º É facultado à interessada 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.

§ 1º 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.

§ 2º 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;

~~§ 3ºOs prazos referidos neste artigo só se iniciam e vencem em dia de expediente no órgão ou na entidade.~~ **REVOGADO**

§ 4ºAssegurado 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; e

IV - o nome ou a razão social do punido, com o número de sua inscrição no Cadastro da Receita Federal.

§ 5º 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.

§ 6º 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 21 de junho 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, ressalvados os casos em que o objeto exija penalidade específica.

Art. 13. As sanções previstas nos artigos 3º, 4º e 5º do presente Decreto serão aplicadas pelo ordenador de despesas do órgão contratante, inclusive nos casos em que o descumprimento recaia sobre o contrato oriundo do Sistema de Registro de Preços.

Art. 14. Os prazos referidos neste Decreto só se iniciam e vencem em dia de expediente no órgão ou na entidade.

Art. 15. Este Decreto entra em vigor na data de sua publicação.

Art. 16. Revogam-se as disposições em contrário.

Brasília,30 de maio de 2006.

118º da República e 47º de Brasília

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 DE 13 DE JULHO DE 2006, P.2.
- 27.069, DE 14 DE AGOSTO DE 2006, PULICADO NO DODF DE 15 DE AGOSTO DE 2006, P. 1, 2.
- 35.831, DE 19 DE SETEMBRO DE 2014, PUBLICADO NO DODF DE 22 DE SETEMBRO DE 2014, P. 6.
- 36.974, DE 11 DE DEZEMBRO DE 2015, PUBLICADO NO DODF DE 14 DE DEZEMBRO DE 2015, P. 7.

DECRETO Nº 26.993, DE 12 DE JULHO DE 2006

DODF DE 13.07.2006

Introduz alterações no Decreto nº 26.851, de 30 de maio de 2006, que "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" (1ª alteração).

A GOVERNADORA DO DISTRITO FEDERAL, no uso das atribuições que lhe confere o artigo 100, inciso VII, da Lei Orgânica do Distrito Federal, DECRETA:

Art. 1º O Decreto nº 26.851, de 30 de maio de 2006, fica alterado como segue:

I – o caput do art. 1º passa a vigorar com a seguinte redação:

"Art. 1º A aplicação das sanções de natureza pecuniária e restritiva de direitos pelo não cumprimento das normas de licitação e/ou de contratos, em face do disposto nos arts. 81, 86, 87 e 88, da Lei Federal nº 8.666, de 21 de junho de 1993, e no art. 7º da Lei Federal nº 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.";

II – o inciso II do art. 3º passa a vigorar com a seguinte redação:

"Art. 3º .....

II - pelo ordenador de despesas do órgão contratante 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.";

III – o caput, o inciso V e o § 2º do art. 4º passam a vigorar com a seguinte redação:

"Art. 4º A multa é a sanção pecuniária que será imposta ao contratado, pelo ordenador de despesas do órgão contratante, por atraso injustificado na entrega ou execução do contrato, e será aplicada nos seguintes percentuais:

.....

V - 20% (vinte por cento) sobre o valor do contrato/nota de empenho, pelo descumprimento de qualquer cláusula do contrato, exceto prazo de entrega.

.....

§ 2º Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá o contratado pela sua diferença, devidamente atualizada pelo Índice Geral de Preços - Mercado (IGP-M) ou equivalente, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrados judicialmente.";

IV – o caput, o inciso II, a alínea c do inciso IV, o inciso II do § 1º e o § 2º do art. 5º, passam a vigorar com a seguinte redação:

"Art. 5° A suspensão é a sanção que impede temporariamente o fornecedor de participar de licitações e de contratar com a Administração, e, se aplicada em decorrência de licitação na modalidade pregão, ainda suspende o registro cadastral da licitante e/ou contratado, no Cadastro de Fornecedores do Distrito Federal, instituído pelo Decreto nº 25.966, de 23 de junho de 2005, e no Sistema de Cadastramento Unificado de Fornecedores - SICAF, de acordo com os prazos a seguir:

.....

II - por até 90 (noventa) dias, em licitação realizada na modalidade pregão presencial ou eletrônico, 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;

.....

IV - .....

c) receber qualquer das multas previstas no artigo anterior e não efetuar o pagamento.

§ 1º .....

II - o ordenador de despesas do órgão contratante, 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.

§ 2º A penalidade de suspensão será publicada no Diário Oficial do Distrito Federal.

.....";

V – o § 1º do art. 6º passa a vigorar com a seguinte redação:

"Art. 6º .....

§ 1º 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 da sanção.

....."

VI – fica revogado o inciso III do art. 7º;

VII – o § 2º do art. 9º passa a vigorar com a seguinte redação, sendo acrescentado o seguinte § 3º, renumerando-se os demais:

"Art. 9º .....

§ 2º Na contagem dos prazos estabelecidos neste Decreto, excluir-se-á o dia do início e incluir-seá o do vencimento, e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário.

§ 3° Os prazos referidos neste artigo só se iniciam e vencem em dia de expediente no órgão ou na entidade.

.....";

VIII – os atuais arts. 13 e 14 ficam renumerados para 14 e 15, ficando inserido o art. 13 com a seguinte redação:

"Art. 13. As sanções previstas nos arts. 3º, 4º e 5º deste Decreto serão aplicadas pelo ordenador de despesas do órgão contratante, inclusive nos casos em que o descumprimento recaia sobre o contrato oriundo do Sistema de Registro de Preços.".

Art. 2º Este Decreto entra em vigor na data de sua publicação.

Art. 3º Revogam-se as disposições em contrário.

Brasília, 12 de julho de 2006

118º da República e 47º de Brasília

MARIA DE LOURDES ABADIA

DECRETO Nº 27.069, DE 14 DE AGOSTO DE 2006

DODF DE 15.08.2006

Altera o Decreto 26.851, de 30 de maio de 2006, que 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 (2ª Alteração).

A GOVERNADORA DO DISTRITO FEDERAL, no uso das atribuições que lhe conferem o inciso VII, art. 100 da Lei Orgânica do Distrito Federal, e tendo em vista o disposto nos arts. 81, 86, 87 e 88 da Lei Federal nº 8.666, de 21 de junho de 1993, e no art. 7º da Lei Federal no 10.520, de 17 de julho de 2002, bem como o disposto no art. 68 da Lei Federal no 9.784, de 29 de janeiro de 1999, e ainda, a centralização de compras instituída nos termos da Lei Distrital no 2.340, de 12 de abril de 1999, e as competências instituídas pela Lei Distrital no 3.167, de 11 de julho de 2003, DECRETA:

Art. 1º O Decreto nº 26.851, de 30 de maio de 2006, fica alterado como segue:

I – o art. 1º passa a vigorar com a seguinte redação:

"Art. 1º A aplicação das sanções de natureza pecuniária e restritiva de direitos pelo não cumprimento das normas de licitação e/ou de contratos, em face do disposto nos arts. 81, 86, 87 e 88, da Lei Federal nº 8.666, de 21 de junho de 1993, e no art. 7º da Lei Federal nº 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 neste Decreto."

II – o art. 2º passa a vigorar com a seguinte redação "Art. 2º As licitantes e/ou contratadas que não cumprirem integralmente as obrigações assumidas, garantida a prévia defesa, estão sujeitas às seguintes sanções:

.....

a) para a licitante e/ou contratada através da modalidade pregão presencial ou eletrônico que, convocada 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 a licitante e/ou contratada será descredenciada 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 as licitantes nas demais modalidades de licitação previstas na Lei nº 8.666, de 21 de junho 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 a contratada 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 a interessada, no respectivo processo, no prazo de 5 (cinco) dias úteis."

III – o art. 3º passa a vigorar com a seguinte redação:

"Art. 3º A advertência é o aviso por escrito, emitido quando a licitante e/ou contratada descumprir qualquer obrigação, e será expedido:

....."

IV – o art. 4º passa a vigorar com a seguinte redação:

"Art. 4º A multa é a sanção pecuniária que será imposta à contratada, pelo ordenador de despesas do órgão contratante, por atraso injustificado na entrega ou execução do contrato, e será aplicada nos seguintes percentuais:

.....

§ 1º A multa será formalizada por simples apostilamento contratual, na forma do art. 65, § 8º, da Lei nº 8.666, de 21 de junho de 1993 e será executada após regular processo administrativo, oferecido à contratada 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 21 de junho de 1993, observada a seguinte ordem:

.....

II - mediante desconto no valor das parcelas devidas à contratada; e

.....

§ 2º Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá à contratada pela sua diferença, devidamente atualizada pelo Índice Geral de Preços - Mercado (IGP-M) ou equivalente, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrados judicialmente.

....."

V – o art. 5º passa a vigorar com a seguinte redação:

"Art. 5º A suspensão é a sanção que impede temporariamente o fornecedor de participar de licitações e de contratar com a Administração, e, se aplicada em decorrência de licitação na modalidade pregão, ainda suspende o registro cadastral da licitante e/ou contratada no Cadastro de Fornecedores do Distrito Federal, instituído pelo Decreto nº 25.966, de 23 de junho de 2005, e 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 - SUCOM, ou pelo órgão integrante do Sistema de Registro de Preços, a licitante e/ou contratada permanecer inadimplente;

....."

VI – o art. 6º passa a vigorar com a seguinte redação:

"Art. 6º A declaração de inidoneidade será aplicada pelo Secretário de Estado ou autoridade equivalente do órgão de origem, à vista dos motivos informados na instrução processual.

§ 1º 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 a contratada ressarcir a Administração pelos prejuízos resultantes de sua conduta e após decorrido o prazo da sanção.

§ 2º 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 21 de junho de 1993."

VII – fica acrescido o parágrafo único ao do art. 7º:

"....

Parágrafo único. Aplicam-se a este artigo as disposições dos §§ 2º e 3º do art. 5º deste Decreto."

VIII – o art. 8º passa a vigorar com a seguinte redação:

"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 21 de junho de 1993 ou 10.520, de 17 de julho de 2002:

....."

IX – o art. 9º passa a vigorar com a seguinte redação:

"Art. 9° É facultado à interessada 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.

.....

§ 6º 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 21 de junho de 1993."

X – o art. 12 passa a vigorar com a seguinte redação:

"Art. 12. Os instrumentos convocatórios e os contratos deverão fazer menção a este Decreto, ressalvados os casos em que o objeto exija penalidade específica."

XI – fica acrescentado o art. 14 com a seguinte redação:

"Art. 14. Os prazos referidos neste Decreto só se iniciam e vencem em dia de expediente no órgão ou na entidade."

II – ficam renumerados os artigos 14 e 15, do Decreto 26.851, de 30 de maio de 2006, para 15 e 16, respectivamente.

Art. 2º Este Decreto entra em vigor na data de sua publicação.

Art. 3º Revogam-se as disposições em contrário, especial o § 3º, do art. 9º, do Decreto 26.851, de 30 de maio de 2006.

Brasília, 14 de agosto de 2006

118º da República e 47º de Brasília

MARIA DE LOURDES ABADIA

DECRETO Nº 35.831, DE 19 DE SETEMBRO DE 2014.

DODF de 22/09/2014

Altera o Decreto nº 26.851, de 30 de maio de 2006, que regula a aplicação de sanções administrativas previstas nas Leis Federais nº 8.666, de 21 de junho de 1993, e nº 10.520, de 17 de julho de 2002, e dá outras providências.

O GOVERNADOR DO DISTRITO FEDERAL, no uso das atribuições que lhe confere o artigo 100, inciso VII e XXVI, da Lei Orgânica do Distrito Federal, DECRETA:

Art. 1º Os incisos I, II e V do art. 4º, do Decreto nº 26.851, de 30 de maio de 2006, passam a vigorar com a seguinte redação:

"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;"

"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;"

"V - até 20% (vinte por cento) sobre o valor do contrato/nota de empenho, pelo descumprimento de qualquer cláusula do contrato, exceto prazo de entrega."

Art. 2º Este Decreto entra em vigor na data de sua publicação.

Art. 3º Revogam-se as disposições em contrário, em especial os incisos I, II e V, do Decreto nº 26.851, de 30 de maio de 2006.

Brasília, 19 de setembro de 2014.

126º da República e 55º de Brasília

AGNELO QUEIROZ

DECRETO Nº 36.974, DE 11 DE DEZEMBRO DE 2015.

DODF de 4/12/2015

Altera o Decreto nº 26.851, de 30 de maio de 2006, que 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.

O GOVERNADOR DO DISTRITO FEDERAL, no uso das atribuições que lhe confere o art. 100, incisos VII e X, da Lei Orgânica do Distrito Federal, DECRETA:

Art. 1º O Decreto nº 26.851, de 30 de maio de 2006, passa a vigorar acrescido do seguinte artigo:

"Art. 4-A A multa de que trata o art. 4º deste Decreto será aplicada, nas contratações previstas na Lei Federal nº 12.232, de 29 de abril de 2010, 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;

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;

III - 1% (um por cento) do valor do contrato em caso de recusa injustificada do adjudicatário em assinar o termo contratual dentro do prazo estabelecido pela Administração;

IV - 1% (um por cento) sobre o valor do contrato que reste executar ou sobre o valor da dotação orçamentária que reste executar, o que for menor, em caso de rescisão contratual;

V - até 1% (um por cento) sobre o valor do contrato que reste executar ou sobre o valor da dotação orçamentária que reste executar, o que for menor, pelo descumprimento de qualquer cláusula do contrato, respeitado o disposto nos incisos I e II."

Art. 2º Este Decreto entra em vigor na data de sua publicação.

Brasília, 11 de dezembro de 2015.

128 da República e 56 de Brasília

RODRIGO ROLLEMBERG

ANEXO VI AO EDITAL

DECLARAÇÃO ACERCA DO DECRETO Nº 7.174, de 12 de maio de 2010.

ÓRGÃO: SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA DO DF.

PROCESSO:

MODALIDADE DE LICITAÇÃO:

NÚMERO DA LICITAÇÃO:

LICITANTE:

CNPJ:

REPRESENTANTE LEGAL:

CPF:

A pessoa jurídica acima identificada, por intermédio de seu representante legal, declara que atende aos requisitos legais estabelecidos em ao menos um dos incisos estabelecidos no art. 5º do Decreto nº 7.174, de 12 de maio de 2010. Essa declaração é a expressão da verdade, sob as penas da lei.

Brasília, _____ de _____ de _____

_____

Assinatura