I – EDITAL SESI-DF Nº: 39/2016

II – REGÊNCIA LEGAL: REGULAMENTO DE LICITAÇÕES E CONTRATOS DO SESI

III – MODALIDADE: PREGÃO ELETRÔNICO

IV – PROCESSO Nº: 015.791/2016

V – TIPO: MENOR PREÇO POR ITEM

VI – FORMA DE FORNECIMENTO: ENTREGA ÚNICA – SESI SEDE – CIF/BRASÍLIA - DF

VII – RECEBIMENTO DAS PROPOSTAS E LANCES:

INÍCIO DO RECEBIMENTO DAS PROPOSTAS: 07 de novembro de 2016.

ENCERRAMENTO DAS PROPOSTAS: 21 de novembro de 2016 (ANTES DA ABERTURA DA SESSÃO DE LANCES).

ABERTURA DA SESSÃO DE LANCES: 21 de novembro de 2016 às 14h (Horário de Brasília).

COMPROVANTE DE ENTREGA DO EDITAL

Recebi do Serviço Social da Indústria - SESI/DF - Departamento Regional do Distrito Federal, o Edital **PREGÃO ELETRÔNICO Nº 39/2016,** tipo **MENOR PREÇO POR ITEM,** cuja realização (abertura da sessão de lances), dar-se-á às **14h (Horário de Brasília),** do **dia 21 de novembro de 2016**, no sítio eletrônico www.pregao.com.br

Objeto: Aquisição de solução de segurança, firewall, para a proteção da rede corporativa, visando atender a demanda da Gerência de Tecnologia da Informação do SESI/DF**,** conforme quantidades e especificações constantes no Anexo II do presente Edital.

RAZÃO SOCIAL: _____

ENDEREÇO: _____

CNPJ: _____

TEL: _____ FAX: _____

E-MAIL: _____

NOME PESSOA PARA CONTATO RESPONSÁVEL: _____

_____CPF:_____

Local de de 2016.

_____

Assinatura

RETIRADA DO EDITAL VIA INTERNET (www.pregao.com.br)

Para formalização do interesse de participar nesta licitação, a empresa deverá repassar este formulário/recibo, devidamente preenchido, para o Serviço Social da Indústria - SESI/DF – Departamento Regional do Distrito Federal, por meio do **e-mail compras@sistemafibra.org.br.**

O Serviço Social da Indústria – SESI/DF - Departamento Regional do Distrito Federal, comunicará as licitantes cadastradas eventuais retificações ocorridas no instrumento convocatório, bem como de quaisquer informações adicionais, no sitio eletrônico: www.pregao.com.br**, ou por meio de correspondência eletrônica.**

A não remessa do recibo, exime o Serviço Social da Indústria – SESI/DF - Departamento Regional do Distrito Federal, da comunicação de eventuais retificações ocorridas no instrumento convocatório, bem como de quaisquer informações adicionais.

I – EDITAL SESI/DF Nº: 39/2016

II – REGÊNCIA LEGAL: REGULAMENTO DE LICITAÇÕES E CONTRATOS DO SESI

III – MODALIDADE: PREGÃO ELETRÔNICO

IV – PROCESSO Nº: 015.791/2016

V – TIPO: MENOR PREÇO POR ITEM

VI – FORMA DE FORNECIMENTO: ENTREGA ÚNICA – SESI SEDE – CIF BRASILIA/DF

VII – RECEBIMENTO DAS PROPOSTAS E LANCES:

INÍCIO DO RECEBIMENTO DAS PROPOSTAS: 07 de novembro de 2016.

ENCERRAMENTO DAS PROPOSTAS: 21 de novembro de 2016, (ANTES DA ABERTURA DA SESSÃO DE LANCES).

ABERTURA DA SESSÃO DE LANCES: 21 de novembro de 2016 às 14h (Horário de Brasília).

1 – DA CONVOCAÇÃO

1.1. O Serviço Social da Indústria - Departamento Regional do Distrito Federal – SESI/DF**,** com sede no SIA Trecho 03, Lote 225, Edifício FIBRA, Brasília/DF, CEP 71.200-030, torna público a todos os interessados que irá realizar licitação na modalidade **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO POR ITEM**, às **14h (Horário de Brasília),** do **dia 21 de novembro de 2016**, na forma estabelecida neste **Edital SESI/DF nº 39/2016** e de acordo com o disposto no Regulamento de Licitações e Contratos do SESI, publicado no DOU de 16/09/1998 com alterações publicadas 26/10/2001, 11/11/2002 e 24/02/2006, e Resolução 1 e 21/2011, de 29/03 e 29/11/11, respectivamente**.**

2 – DO OBJETO

2.1. Aquisição de solução de segurança, firewall, para a proteção da rede corporativa, visando atender a demanda da Gerência de Tecnologia da Informação do SESI/DF, conforme quantidades e especificações constantes no Anexo II do presente Edital.

2.2. O Edital e seus Anexos poderão ser retirados por meio do sitio**:** www.pregão.com.br ou na Coordenação de Aquisição, localizada no seguinte endereço: SIA Trecho 3, Lote 225, Subsolo, Edifício FIBRA, Brasília/DF, CEP: 71.200-030.

3 – DO PRAZO E DO LOCAL DE ENTREGA.

3.1. Do Prazo de Entrega: Em até **30 (trinta) dias,** contados a partir da assinatura do Pedido de Compra.

3.2. Local de Entrega: Gerência de Tecnologia da Informação do SESI/DF, SIA Trecho 3, Lote 225, Edifício FIBRA, Brasília/DF CEP: 71200-030, Telefone: (61) 3362-6018, contato: Diego Rosa.

4 – DA PARTICIPAÇÃO

4.1. Somente poderão participar deste Pregão Eletrônico, as empresas legalmente estabelecidas no território nacional, de ramo compatível com o objeto desta licitação, que satisfaçam as condições e as exigências do presente Edital, inclusive quanto à regularidade da documentação, e que estejam devidamente cadastradas junto ao Órgão Provedor do Sistema, através do portal www.pregao.com.br.

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

4.2. Não será admitida nesta licitação a participação de empresas:

4.2.1. Estejam sob decretação de falência, concordata, recuperação judicial ou extrajudicial (conforme Lei nº 11.101/2005), dissolução ou liquidação.

4.2.2. Que estejam com o direito de licitar e/ou contratar com o SESI/DF suspenso ou que por este tenham sido declaradas inidôneas.

4.2.3. Tenham participação, a que título for, de dirigentes ou empregados do SESI/DF.

4.3. Estarão impedidas de participar da licitação, direta ou indiretamente:

4.3.1. Empregado, dirigente ou Conselheiro do SESI/DF.

4.3.2. Empresas que tenham entre seus dirigentes, gerentes, sócios e/ou responsáveis técnicos empregados, dirigentes, Conselheiro, membro titular ou suplente da Comissão de Licitação do SESI/DF.

4.3.3. Empresas que tenham entre seus dirigentes, gerentes, sócios e/ou responsáveis técnicos cônjuge ou parente até segundo grau de empregados, dirigentes ou Conselheiro do SESI/DF.

5 – DA REPRESENTAÇÃO E DO CREDENCIAMENTO

5.1. Para participar deste Pregão Eletrônico, os interessados deverão procurar a Bolsa de Mercadorias de sua região. Em Brasília, BBSB (Bolsa de Brasília) sito à SCS Quadra 6, Edifício Citybank, Bloco A, 2º andar, telefone: (61) 3224-9731, BNM (Bolsa Nacional de Mercadorias), sito à SEUPN 513, Bloco B, Edifício Imperador, Salas 102/104, telefone: (61) 3340-8912 e BBEN (Bolsa Brasileira Eletrônica de Negócios), sito à SIBS Quadra 01, Conjunto A, 05 – Parte, Núcleo Bandeirante, telefone: (61) 3386-1017 ou 3327-1557 que lhe prestará o apoio técnico e operacional em todas as fases do certame.

5.1.1. Poderão representar a licitante em todo o processo que envolve a licitação, os Agentes de Negócios devidamente credenciados em uma Bolsa de Mercadorias.

5.2. Para participar deste Pregão Eletrônico, o interessado, por meio do seu Agente de Negócios, deverá ser cadastrado no Sistema de Interligação de Bolsas Brasileiras, no endereço www.pregao.com.br, até o momento anterior à abertura das Propostas/Início da sessão pública de lances.

5.2.1. As licitantes somente poderão se fazer representar por intermédio de um único Agente de Negócios para o Edital do **Pregão Eletrônico SESI/DF Nº 39/2016**.

5.2.2. A representação deverá ser formalizada por procuração pública ou particular, com firma reconhecida, acompanhada de cópia do ato de investidura do outorgante, no qual conste expressamente ter poderes para devida outorga.

5.3. O interessado, ao se cadastrar no Portal, terá o seu credenciamento efetivado pela atribuição de chave de identificação e de senha pessoal e intransferível, para acesso ao sistema eletrônico.

5.3.1. O credenciamento do interessado, junto ao provedor do sistema, implica a responsabilidade legal da Licitante ou seu Agente de Negócios e a presunção de sua capacidade técnica para realização das transações inerentes ao sistema eletrônico.

5.3.2. O uso da senha de acesso ao sistema eletrônico é de inteira responsabilidade da Licitante ou seu Agente de Negócios, não cabendo ao provedor do sistema ou à promotora da licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

6 – DA IMPUGNAÇÃO AO EDITAL

6.1. Qualquer pessoa poderá, **até 02 (dois) dias úteis anteriores a data de abertura**, impugnar o ato convocatório do certame por meio do sítio eletrônico www.pregao.com.br, na opção “Recursos”, “Impugnar Edital”.

6.2. Caberá a Pregoeira encaminhar o assunto acompanhado de parecer à Autoridade Superior a quem compete decidir sobre a petição no prazo de **24h (vinte e quatro horas).**

6.3. Acolhida a petição contra o ato convocatório ou havendo necessidade de prazo maior para julgamento da questão, nova data será designada pela Pregoeira para a realização do certame, informando as licitantes por meio do sistema.

7 – DO ENVIO DA PROPOSTA DE PREÇOS

7.1. A licitante será responsável por todas as transações que forem efetuadas, em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas.

7.2. A participação no Pregão Eletrônico dar-se-á por meio da digitação da senha privativa de acesso ao sistema, do cadastramento da licitante no Cadastro de Participantes para o Edital/Item e subsequente cadastramento da Proposta de Preços com valor total, a partir do dia da publicação do Edital no jornal e/ou Internet, exclusivamente por meio do sistema eletrônico www.pregao.com.br/licitante**.**

7.3. A Proposta de Preços, constante no Anexo II deste Edital, deverá ser anexada à Proposta Eletrônica no ato do seu cadastramento no sistema, cujos valores informados deverão serem idênticos.

7.3.1. A Proposta de Preços constante no Anexo II, deverá conter preço unitário e total para o item nela constante, em Real (R$), em algarismos arábicos em até 2 (duas) casas decimais, fixos e irreajustáveis durante o prazo de validade da proposta, contados a partir da abertura da sessão de lances do Pregão, bem como valor global da proposta expresso em algarismo e por extenso.

7.4. Deverá constar na proposta de preços a marca do item cotado.

7.5. Na Proposta de Preços formulada em conformidade ao Anexo II deste Edital, devem estar previstos todos os custos diretos e indiretos pertinentes à formação dos preços do objeto, incluindo despesas com tributos, fretes e entregas, seguros, taxas e demais encargos, não sendo lícita a cobrança posterior de qualquer ônus, ficando a licitante obrigada a fornecer o objeto pelo valor resultante de sua Proposta.

7.6. Apresentar, declaração expressa da garantia mínima de 3 (anos) anos, contra defeitos de fabricação para o item ofertado, a partir da data de emissão da nota fiscal, conforme modelo constante do Anexo V deste Edital.

7.7. Como requisito para a participação no certame a licitante deverá manifestar, em campo próprio do sistema eletrônico, o pleno conhecimento e atendimento às exigências de habilitação, bem como as especificações técnicas descritas no Edital e seus Anexos.

7.8. A licitante vencedora fica obrigada a garantir a qualidade do firewall ofertado, quando da entrega do objeto licitado, obrigando-se a substituí-lo, imediatamente, caso esteja fora do padrão, sem quaisquer ônus para este SESI/DF, até o efetivo atendimento da referida proposta.

7.9. As licitantes deverão informar, na Proposta de Preços correspondente ao Anexo II deste Edital, o nome do banco, o código da agência e o número da conta corrente da empresa, para efeito de pagamento, bem como os dados do responsável pela assinatura do Instrumento Contratual (nome completo, nº do documento de identidade, nº do CPF, estado civil, nacionalidade, endereço completo, profissão, cargo que exerce na empresa e e-mail).

7.10. Prazo de validade da proposta, não será inferior a **60 (sessenta) dias corridos**, a contar da data da abertura da sessão de lances.

7.11. A apresentação da proposta implicará plena aceitação, por parte da proponente, de todas as condições estabelecidas neste Edital e seus Anexos.

7.12. A licitante vencedora fica obrigada a apresentar a Proposta de Preços, correspondente ao Anexo II deste Edital, no prazo máximo de 48h (quarenta e oito horas), com as especificações detalhadas do objeto ofertado, bem como com os valores readequados ao valor total representado pelo lance vencedor, devendo, para tanto, encaminhá-la à Coordenação de Aquisição do SESI/DF, localizada no SIA Trecho 3, Lote 225, Subsolo, Edifício FIBRA, Brasília/DF CEP: 71.200-030. No verso do envelope que irá conter este documento, deve-se fazer referência ao Edital de PREGÃO ELETRÔNICO SESI/DF Nº 39/2016.

7.13. Serão desclassificadas as propostas de preços que não atenderem às exigências do presente Edital e seus Anexos, quer sejam por omissão ou por apresentarem irregularidades insanáveis.

8 – DA DIVULGAÇÃO DAS PROPOSTAS DE PREÇOS

8.1. A partir das **14h** do **dia 21 de novembro de 2016** e em conformidade com o Item 5 deste Edital, será aberta a sessão pública do **Pregão Eletrônico SESI Nº 39/2016**, com a divulgação pela Pregoeira através do sistema, das Propostas de Preços recebidas e início da etapa de lances.

9 – DA ACEITABILIDADE DA PROPOSTA

9.1. Os preços constantes no Anexo I – Planilha Estimativa de Preços correspondem à referência de preço máximo a que o SESI/DF está disposto a pagar pelo objeto da licitação.

9.2. A apresentação de proposta com valor acima do estimado pelo SESI/DF, não implicará na sua desclassificação automática, sendo facultado à licitante a readequação dos valores por meio da oferta de lances sucessivos.

9.3. Caso à Licitante classificada não ofereça lances dentro do estimado pelo SESI/DF, o respectivo item da proposta de preços será automaticamente CANCELADO.

10 – DA FORMULAÇÃO DOS LANCES

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

10.2. Iniciada a etapa competitiva, as licitantes com propostas aceitas poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do recebimento e do valor do lance.

10.3. As licitantes poderão oferecer lances sucessivos, desde que observado o horário fixado e as regras de aceitação dos mesmos.

10.4. Somente serão aceitos pelo sistema, os lances cujos valores forem inferiores ao último lance que tenha sido anteriormente ofertado pela própria licitante e registrado no sistema, em intervalos de valor definidos pela Pregoeira.

10.4.1. Durante a Etapa de Lances da Sessão Pública, o sistema registrará o lance acima do menor lance ofertado, desde que este seja inferior ao último lance encaminhado pelo próprio ofertante. Essa possibilidade prevista na legislação permitirá a disputa pelo segundo, terceiro, quarto lugares, sucessivamente.

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

10.6. Durante o transcurso da sessão pública de Pregão, as licitantes serão informadas, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelas demais licitantes, vedada à identificação do detentor do lance.

10.7. No caso de desconexão com a Pregoeira no decorrer da sessão de lances do Pregão, o sistema eletrônico poderá permanecer acessível às licitantes para a oferta dos lances.

10.7.1. A Pregoeira, quando possível, dará continuidade a sua atuação no certame, sem prejuízo dos atos realizados.

10.7.2. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão de lances do Pregão será suspensa e terá reinício somente após comunicação expressa da Pregoeira aos participantes.

10.8. A critério da Pregoeira, o sistema eletrônico emitirá aviso de que terá início o prazo aleatório de até 30 (trinta) minutos para o encerramento da fase de lances, findo o qual estará automaticamente encerrada a recepção de lances.

10.9. O fechamento do certame, pela Pregoeira, será precedido de 3 (três) mensagens de marteladas. O intervalo de tempo entre uma martelada e outra terá duração de, no mínimo, 3 (três) segundos entre elas. Entre o intervalo de cada martelada, a Pregoeira enviará nova mensagem aos participantes solicitando novos lances. Se algum participante ofertar novo lance, a contagem das marteladas será zerada, recomeçando o fechamento. Com a terceira martelada, o item é negociado pelo valor do último lance.

10.10. Após o encerramento do **Pregão Eletrônico SESI/DF Nº 39/2016**, a Pregoeira deverá divulgar por meio do sistema o nome da Licitante classificada para o Item.

10.11. Encerrada a etapa de lances da sessão pública, a licitante detentora da menor oferta deverá comprovar a situação de regularidade (documentação de habilitação), devendo, para tanto, encaminhá-la, no prazo máximo de 2 (dois) dias úteis, dentro de envelope lacrado, endereçado à Coordenação de Aquisição do SESI/DF, localizada no SIA Trecho 3, Lote 225, Edifício FIBRA, Subsolo, Brasília/DF, CEP: 71.200-030. No verso do envelope que irá conter esta documentação, a licitante vencedora deverá fazer referência ao número do Edital de PREGÃO ELETRÔNICO SESI/DF Nº 39/2016.

10.11.1. Os documentos a serem apresentados para cumprimento das exigências são os relacionados no Item 12 deste Edital.

11 – DO JULGAMENTO DAS PROPOSTAS DE PREÇOS

11.1. Se a proposta de menor preço não for aceitável ou se a licitante desatender às exigências da habilitação, a Pregoeira examinará a proposta subsequente, verificando a sua aceitabilidade e procedendo à sua habilitação, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda ao Edital.

11.1.1. Ocorrendo situação a que se refere o subitem acima, a Pregoeira poderá negociar com a licitante para que seja obtido preço melhor.

11.2. Da decisão que desclassificar as propostas de preços, somente caberá pedido de reconsideração à própria comissão a ser apresentado exclusivamente por meio do sistema eletrônico, acompanhado da justificativa de suas razões, no prazo máximo de 30 (trinta) minutos a contar do momento em que vier a ser disponibilizada no sistema eletrônico.

12 – DA HABILITAÇÃO

12.1. A habilitação da Licitante classificada será verificada mediante apresentação dos seguintes documentos:

12.1.1. Quanto à Habilitação Jurídica:

a) Registro Comercial, no caso de empresa individual, acompanhado da cédula de identidade do proprietário.

b) Ato Constitutivo, Estatuto ou Contrato Social em vigor com todas as suas respectivas alterações ou Contrato Social consolidado, devidamente registrado, em se tratando de sociedades comerciais. No caso de sociedade por ações e/ou cooperativas, deverá ser apresentado, ainda, documento de eleição de seus administradores.

c) Inscrição do Ato Constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício; a em funcionamento no país e ato de registro ou autorização para funcionamento expedido.

d) Decreto de Autorização, em se tratando de empresa ou sociedade estrangeiro pelo órgão competente, quando a atividade assim o exigir.

e) **Certidão Simplificada da Junta Comercial do Distrito Federal ou do Estado ou certidão emitida pelo Cartório de Ofício de Pessoas Jurídicas, dentro do prazo de validade ou expedida no prazo máximo de 6 (seis) meses, conforme o caso.**

12.1.2. Quanto à Regularidade Fiscal:

a) Prova de Inscrição no Cadastro Nacional das Pessoas Jurídicas – CNPJ.

b) Prova de Inscrição no Cadastro de Contribuintes Estadual e municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual.

c) Prova de Regularidade junto ao Fundo de Garantia por Tempo de Serviço – CR/FGTS, emitido pela Caixa Econômica Federal.

d) Prova de Regularidade para com a Fazenda Federal, Estadual e Municipal, se houver, do domicílio ou sede da licitante, mediante apresentação de:

d.1.) Prova de Regularidade Fiscal, perante a Fazenda Nacional, relativa aos Tributos e Contribuições Federais e à Dívida Ativa da União, emitida pela Secretaria da Receita Federal do Brasil.

d.2) Prova de Regularidade junto à Secretaria da Fazenda e Planejamento do Governo do Distrito Federal (para as empresas sediadas em Brasília).

d.3.) Prova de Regularidade para com as Fazendas Estadual ou Municipal (para as empresas sediadas em outras localidades).

12.1.3. Quanto a Regularidade Trabalhista:

a) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas – CNDT, CONFORME Lei federal nº 12440/2011, dentro do prazo de validade.

12.1.4. Quanto a Qualificação Econômico-Financeira:

a) Certidão negativa de falência, concordata ou recuperação judicial ou extrajudicial, expedida pelo distribuidor da sede da pessoa jurídica, dentro do prazo de validade. Nos casos em que não houver validade na própria certidão, esta deverá ter sido emitida há, no máximo, 3 (três) meses.

12.1.5. Quanto à Qualificação Técnica

a) Apresentação de atestado(s) ou certidão(ões) de capacidade técnica, fornecidos por pessoas jurídicas de direito público ou privado, no(s) qual(is) deverá restar comprovado que a empresa participante forneceu ou fornece os itens compatíveis em características ao objeto desta licitação.

a.1) A comprovação que se refere à alínea acima se dará por meio de atestado ou certidão, fornecido por pessoa jurídica de direito público ou privado, contendo as seguintes informações:

a. Nome ou razão social, CNPJ e endereço completo do emitente;

b. Nome ou razão social da empresa para quem forneceu ou fornece o objeto;

c. Data de emissão do atestado ou da certidão;

d. Assinatura e identificação do signatário (nome, telefone, cargo e função que exerce junto à empresa emitente).

b) O SESI/SENAI-DF poderá exigir da proposta melhor classificada à apresentação de cópia autenticada da Nota Fiscal ou Instrumento Contratual que deram origem ao Atestado.

12.1.6. Outros documentos:

a) Declaração de que não emprega menor, conforme modelo constante no Anexo IV do presente Edital.

12.2. A documentação acima elencada deverá ser apresentada em conformidade ao disposto no subitem 10.11.

12.3. Os documentos mencionados acima poderão ser apresentados em cópia simples, acompanhado do original para autenticação pela Pregoeira ou por qualquer processo de cópia devidamente autenticada por tabelião de notas (Cartório) ou impressos por meio de pesquisa feita nos sítios eletrônicos dos órgãos oficiais emitentes dos referidos documentos, os quais deverão estar em perfeitas condições de legibilidade e entendimento.

12.4. Os documentos deverão ser apresentados em envelope, opaco, fechado de forma indevassável e rubricados em suas partes coladas com a seguinte inscrição Serviço Social de Indústria – SESI/DF - Departamento Regional do Distrito Federal – **Pregão Eletrônico SESI/DF Nº 39/2016**.

12.5. A licitante poderá entregar a Pregoeira o envelope da documentação ou apresentá-lo por meio do Agente de Negócios credenciado, habilitado na forma do Item 5 deste Edital.

12.6. Não serão aceitos “protocolos de entrega” ou “solicitação de documento” em substituição aos documentos requeridos no presente Edital e seus Anexos.

12.7. Sob pena de inabilitação, os documentos acima referenciados deverão estar em nome da licitante e conter o mesmo número do CNPJ, que deverá corresponder ao CNPJ constante da proposta da licitante. Se a licitante for a matriz, todos os documentos deverão estar em nome da matriz; e se a licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

12.8. Todos os documentos emitidos em língua estrangeira deverão ser entregues acompanhados da tradução para a língua portuguesa, efetuada por Tradutor Juramentado, e também devidamente consularizados ou registrados no Cartório de Títulos e Documentos. Documentos de procedência estrangeira, mas emitidos em língua portuguesa, também deverão ser apresentados devidamente consularizados ou registrados no Cartório de Títulos e Documentos.

12.9. Serão inabilitadas a(s) empresa(s) que não atender(em) ao Item 12 deste Edital.

13 – DOS RECURSOS ADMINISTRATIVOS

13.1. Declarado o vencedor, qualquer licitante poderá manifestar motivadamente a intenção de recorrer, **no prazo máximo de 24h (vinte e quatro horas) exclusivamente** por meio do sítio eletrônico **www.pregao.com.br**. Neste caso, ser-lhe-á concedido o prazo de mais 2 (dois) dias úteis para apresentação das razões do recurso, ficando as demais licitantes desde logo intimadas para apresentar contrarrazões em igual número de dias, que começarão a correr a partir do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

13.2. A decisão da Pregoeira sobre o recurso deverá ser motivada e submetida à apreciação da autoridade superior a quem compete decidir sob a petição.

13.3. A falta de manifestação imediata e motivada da licitante importará a decadência do direito de recurso e adjudicação do objeto pela Pregoeira ao vencedor.

13.4. O recurso contra decisão da Pregoeira não terá efeito suspensivo.

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

13.6. Os recursos deverão ser interpostos **exclusivamente** por meio do site **www.pregao.com.br.**

13.7. Não serão conhecidos os recursos interpostos após o referenciado prazo, bem como os que forem enviados por fax ou e-mail.

13.8. Os autos do processo permanecerão com vista franqueada aos interessados, na Coordenação de Aquisição do SESI/DF, localizada no SIA Trecho 03, Lote 225, Subsolo, Edifício FIBRA, Brasília/DF, CEP 71.200-030.

14 – DA ADJUDICAÇÃO E HOMOLOGAÇÃO

14.1. A adjudicação do objeto do presente certame será viabilizada pela Pregoeira designada, sempre que não houver recursos.

14.2. A homologação da licitação é de responsabilidade do Gerente de Administração e Finanças e do Superintendente do SESI/DF e só poderá ser realizada depois da adjudicação do objeto à proponente vencedora pela Pregoeira.

15 – DA ASSINATURA DO PEDIDO DE COMPRA – PED

15.1. Este instrumento contratual será emitido pelo sistema eletrônico da entidade. As condições nele dispostas são as mesmas constantes neste instrumento convocatório.

15.2. Independentemente de sua transcrição, para todos os efeitos legais, farão parte do Pedido de Compra - PED que vier a ser assinado todas as condições estabelecidas no presente Edital e seus Anexos, na "**PROPOSTA DE PREÇOS"** e na **"DOCUMENTAÇÃO DE HABILITAÇÃO"** da licitante vencedora.

15.3. A empresa vencedora fica obrigada a aceitar, nas mesmas condições pactuadas, os acréscimos ou decréscimos que se fizerem necessários, até 25% (vinte e cinco por cento) do valor inicial do Instrumento Contratual atualizado, conforme Artigo 30 do Regulamento de Licitações e Contratos do SESI.

15.4. A licitante vencedora deverá comparecer ao SESI/DF, no prazo máximo de **05 (cinco) dias**, contados de sua convocação, para a assinatura do Pedido de Compra - PED.

15.5. A vigência do Pedido de Compra será de **3 (três) meses** a contar da data de assinatura.

16 – OBRIGAÇÕES DA CONTRATADA

16.1. Constituem obrigações da CONTRATADA, independentemente de outras decorrentes do presente instrumento, da proposta apresentada e das normas e disposições constantes do Regulamento de Licitações e Contratos do SESI, que o regem:

16.1.1. Entregar o firewall, conforme as condições e especificações técnicas solicitadas neste Edital.

16.1.2. Entregar o firewall, embalado e protegido de forma adequada, contra manuseio e transporte, no local e prazo estipulado neste Edital, acompanhados da respectiva nota fiscal.

16.1.3. Responsabilizar-se, no que se refere ao pessoal empregado na entrega do firewall pelo cumprimento integral das prescrições referentes às leis tributárias, trabalhistas, previdenciárias e de segurança do trabalho, cujos encargos lhe caberá responder unilateralmente em toda a sua plenitude.

16.1.4. Arcar com todas as despesas relativas a entrega do firewall descritos neste Edital, tais como taxas, tributos, impostos, encargos sociais, seguros, despesas com transporte e demais gastos e custos inerentes ao cumprimento deste objeto.

16.1.5. Assumir todos os encargos de possíveis demandas cíveis e penais relacionadas à entrega do firewall, originariamente ou vinculada por prevenção, conexão ou continência.

16.1.6. Emitir nota fiscal do firewall fornecido, ficando vedada a inclusão de item adverso aos contratado na mesma nota fiscal.

16.1.7. Responder por quaisquer danos pessoais ou materiais causados por seus empregados ao SESI/DF ou a terceiros decorrentes da execução do objeto.

16.1.8. Comunicar por escrito, e imediatamente, ao Gestor do Instrumento Contratual qualquer motivo que impossibilite o fornecimento do firewall nas condições pactuadas.

16.1.9. Responsabilizar-se por todas as despesas em caso de devolução do firewall por estar em desacordo com as especificações técnicas descritas neste Edital.

16.1.10. Respeitar as normas e procedimentos de controle e acesso às dependências do SESI/DF.

16.1.11. Assumir o compromisso de indenizar o SESI/DF, independentemente da continuidade da vigência do Instrumento Contratual a ser celebrado entre esta entidade e a empresa Contratada, por eventual condenação judicial em processo que envolva qualquer um dos profissionais designados para a operacionalização do ajuste ou terceiros envolvidos.

16.1.12. Prestar garantia mínima de 03 (três) anos do fabricante, contatos a partir da emissão da nota fiscal.

17 – DAS OBRIGAÇÕES DO SESI

17.1. Efetuar os pagamentos devidos, de acordo com o estabelecido neste Edital, no prazo de **até 30 (trinta) dias**, contados do aceite da nota fiscal/fatura pela área demandante, desde que respeitadas às condições e quantidade pactuado.

17.2. Verificar a regularidade de recolhimento dos encargos sociais e trabalhistas antes do pagamento.

17.3. Proporcionar à Contratada todas as condições necessárias ao cumprimento das obrigações decorrentes deste Edital, devendo especificar os detalhes necessários à perfeita entrega do seu objeto.

17.4. Promover, através de seu representante, o acompanhamento e a fiscalização do Instrumento Contratual, sob os aspectos quantitativo e qualitativo, anotando em registro próprio as falhas detectadas e comunicando à Contratada as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas.

17.5. Recusar o objeto, caso não estejam de acordo com as especificações técnicas deste Edital, correndo por conta da empresa Contratada todas as despesas, referente ao recolhimento do objeto.

17.6. Comunicar à Contratada toda e qualquer ocorrência relacionada com a entrega do objeto.

17.7. Notificar a Contratada, sobre toda e qualquer ocorrência, imperfeições, falhas ou irregularidades constatadas durante a entrega do firewall, para que sejam adotadas medidas corretivas necessárias.

17.8. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos empregados da Contratada.

18 – DA FORMA DE PAGAMENTO

18.1. A empresa contratada apresentará nota fiscal, em 2 (duas) vias, acompanhada da documentação constante do subitem 12.1.2: letra “a” (**CNPJ**), letra “b” **(Prova de Inscrição no Cadastro de Contribuintes Estadual ou Municipal – compatível com o objeto social),** letra “c” (**CR/FGTS**), letra “d.1” (**CERTIDÃO DE QUITAÇÃO DE TRIBUTOS E CONTRIBUIÇÕES FEDERAIS/INSS**), letra “d.2” (**CERTIDÃO DE REGULARIDADE DO GDF – para as empresas sediadas em Brasília)** e “d.3” (**CERTIDÃO DE REGULARIDADE ESTADUAL E MUNICIPAL – para as empresas sediadas em outra localidades)** deste Edital, para liquidação e pagamento da despesa contraída pelo SESI/DF.

18.2. A empresa contratada estará sujeito as retenções tributárias legais, devendo o mesmo informar no corpo da Nota Fiscal às deduções as quais ele se adequa.

18.3. Após o recebimento e aceite do objeto do presente Edital, o crédito será efetuado em conta bancária em nome da licitante vencedora, devendo os dados serem informados no corpo da Nota Fiscal, contados do aceite pela Gerência de Tecnologia da Informação do SESI/DF, conforme cronograma de desembolso constante do Anexo III deste Edital.

18.4. Após recebimento definitivo do objeto licitado, o pagamento será efetuado, em parcela única, **em até 30 (trinta) dias**, contados do aceite da Nota Fiscal/Fatura pela Gerência de Tecnologia da Informação do SESI/DF.

18.5. Para liquidação dos valores relativos a entrega do firewall será ainda observado o que segue:

18.5.1. Reserva-se no direito de recusar o pagamento se o objeto deste edital não for entregue, de acordo com o proposto, aceito e pactuado.

18.5.2. Poderá deduzir do montante a pagar, as indenizações devidas pela empresa Contratada, em razão da inadimplência nos termos do Instrumento Contratual que vier a ser firmado.

18.5.3. A aprovação das Notas Fiscais fica condicionada ao recebimento definitivo que dar-se-á após a conferência e aceitação do firewall para fins de confirmação com as especificações técnicas descritas no Anexo II deste Edital, podendo o SESI/DF rejeitar, no todo ou em parte, a entrega executada em desacordo.

18.5.4. As Notas Fiscais não aprovadas pelo SESI/DF serão devolvidas à Contratada, para as devidas correções, acompanhadas dos motivos de sua rejeição, recontando-se para pagamento o prazo estabelecido no subitem 18.4. deste Edital, a partir da sua reapresentação, sem qualquer tipo de correção de seu valor, sendo automaticamente alteradas as datas de vencimento, não respondendo o proponente do Edital por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.

19 – DAS PENALIDADES

19.1. Salvo hipótese de caso fortuito ou de força maior, a inexecução total ou parcial injustificada, a execução deficiente, irregular ou inadequado do objeto deste Edital, assim como o descumprimento dos prazos e condições estipulados, implicará na aplicação das penalidades abaixo explicitadas.

19.2. Caso a licitante vencedora se recuse injustificadamente a retirar e assinar o Instrumento Contratual, dentro do prazo máximo, ou declinar da proposta, ficará caracterizado o descumprimento total da obrigação assumida, ficando a vencedora sujeita à aplicação das penalidades abaixo explicitadas, a seguir descritas, isolada ou cumulativamente, com determinação e grau de aplicação a critério do SESI/DF:

a) Advertência.

b) Multa.

c) Suspensão temporária de participação em licitações e impedida de contratar com o Sistema FIBRA, por prazo não superior a **2 (dois) anos.**

19.3. Caso a licitante vencedora não aceitar, receber e assinar o Instrumento Contratual no prazo estipulado, este deverá ser anulado, sujeitando-se a licitante faltosa à multa de 10% (dez por cento) calculado sobre o valor considerado em sua proposta, sem prejuízo das demais sanções.

19.4. Ocorrendo atraso na entrega do objeto desta licitação, salvo por motivo de força maior devidamente reconhecido e aceito pelo Sistema FIBRA/DF, ficará a licitante contratada sujeita à multa mensal de 2% (dois por cento) sobre o valor da fatura a pagar, mais 1% (um por cento) de mora, sem prejuízo das demais penalidades.

19.5. No caso de aplicação de qualquer das multas previstas no Edital, estas serão descontadas de qualquer fatura ou crédito existente em favor da licitante Contratada.

19.6. A prática de atos ilícitos em quaisquer das fases desta licitação implicará na suspensão do direito de licitar com o Sistema FIBRA por prazo de até **02 (dois) anos.**

19.7. Para aplicação das penalidades aqui previstas, a empresa Contratada será notificada para apresentar defesa prévia no prazo máximo de **05 (cinco) dias úteis**, contados da sua notificação.

19.8. As penalidades previstas neste edital são independentes entre si, podendo ser aplicadas isolada ou cumulativamente, sem prejuízo de outras medidas cabíveis.

20 – DAS DISPOSIÇÕES GERAIS

20.1. O SESI/DF não admitirá declarações posteriores ao recebimento dos envelopes de "PROPOSTA DE PREÇOS" e "DOCUMENTAÇÃO DE HABILITAÇÃO", de desconhecimento de fatos, no todo ou em parte, nem juntadas de documentos fora das datas especificadas neste Edital, que dificultem ou impossibilitem o julgamento das propostas ou a adjudicação à licitante vencedora.

20.2. É parte integrante deste Edital, os seguintes Anexos:

- ANEXO I – PLANILHA ESTIMATIVA DE PREÇOS.

- ANEXO II – FORMULÁRIO DE PROPOSTA DE PREÇOS.

- ANEXO III – CRONOGRAMA DE DESEMBOLSO FINANCEIRO.

- ANEXO IV – DECLARAÇÃO DE QUE NÃO EMPREGA MENOR.

- ANEXO V –DECLARAÇÃO DE GARANTIA DO EQUIPAMENTO.

20.3. É facultado a Pregoeira, em qualquer fase da licitação, promover diligência destinada a esclarecer ou a complementar a instrução do processo, vedada inclusão posterior de documento ou informação que deveria constar originariamente na PROPOSTA DE PREÇOS e na DOCUMENTAÇÃO DE HABILITAÇÃO.

20.4. Decairá do direito de impugnar os termos deste Edital, perante o SESI/DF, a licitante que não o fizer até 02 (dois) dias úteis anteriores à data de abertura, quanto a eventuais falhas ou irregularidades do Edital, hipótese em que tal comunicação não terá efeito de recurso.

20.5. Qualquer pedido de esclarecimento sobre este Edital deverá ser encaminhado, por escrito, a Pregoeira, entregue e protocolado no SIA Trecho 03, Lote 225, Edifício FIBRA, Brasília/DF, CEP 71.200-030, ou pelo e-mail: **compras@sistemafibra.org.br**, até **02 (dois) dias úteis** anteriores à data de abertura.

20.6. Os empregados e prepostos da empresa Contratada não terão qualquer vínculo empregatício com o SESI/DF, correndo por conta exclusiva da licitante vencedora todas as obrigações decorrentes das legislações trabalhista, previdenciária, fiscal, tributária e comercial, as quais a licitante vencedora se obriga a saldar na época devida.

20.7. É facultado ao SESI/DF, quando a convocada não assinar o Instrumento Contratual, dentro do prazo de que trata o subitem 15.2, convocar as licitantes remanescentes, observadas a ordem de classificação para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado, inclusive quanto aos preços ou ainda cancelar a licitação.

20.8. Fica assegurado ao SESI/DF o direito de cancelar a presente licitação mediante justificativa, antes da assinatura do Instrumento Contratual, sem que, em decorrência dessa medida tenham as licitantes direito à indenização, à compensação ou à reclamação de qualquer natureza.

20.9. O foro da Circunscrição Especial Judiciária de Brasília, Distrito Federal, será o competente para dirimir as questões oriundas desta Licitação e da relação jurídica dela decorrente.

20.10. Os casos omissos deste Edital serão resolvidos pela Pregoeira e pela Equipe de Apoio, com aplicação das disposições contidas no Regulamento de Licitações e Contratos do SESI.

Brasília – DF, 07 de novembro de 2016

PATRICIA DE CASTRO MACHADO GOMES
Pregoeira

ANEXO I – PLANILHA ESTIMATIVA DE PREÇOS

ITEM	UN.	QTD	PRODUTO	VALOR ESTIMADO UNITÁRIO	VALOR ESTIMADO TOTAL
01	UN.	01	**FIREWALL** **Especificações técnicas mínimas:** **Especificação Geral:** • Aquisição de solução de proteção de rede para segurança de informação perimetral, firewall, que inclua filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares, Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta. • Por plataforma de segurança entende-se hardware e software integrados do tipo appliance. **Capacidade, atendendo aos seguintes requisitos mínimos:** • A plataforma de segurança deverá possuir a capacidade e as características abaixo: • Funcionalidade de Firewall com throughput de no mínimo 12 GBps. • Appliance deve suportar throughput de no mínimo 2 GBps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS, antivírus e antispyware. • Suportar no mínimo, 4.000.000 de conexões simultâneas. • Suportar no mínimo, 65.000 novas conexões por segundo. • Suportar no mínimo 2000 usuários simultâneos com todas as características do item 2.1.2 habilitadas. • Fonte 120/240 AC. • 06 (seis) interfaces de rede 10/100/1000 base-TX.	R$ 114.400,39	R$ 114.400,39

			• 1 (uma) interface do tipo console ou similar para configuração e manutenção. • Deve suportar e estar licenciada para uso de no mínimo 50 (cinquenta) clientes de VPN SSL simultâneos. • Deve suportar o thoughput de 2 Gbps de VPN e 2 Gbps de IPS. • Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento. • A console de gerência e monitoração local pode residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função. **Características Gerais:** • O equipamento deverá ser novo e estar em linha de produção na data do edital. Não serão aceitos equipamentos que já tenham anuncio de fim de vida. • A solução deve consistir de appliance de proteção de rede com funcionalidades de UTM ou NGFW e console de gerência e monitoração. • Por funcionalidade de segurança entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões. • O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. • Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. • O equipamento fornecido deve ser próprio para montagem em rack 19” acompanhado dos kits de instalação ou deverá ser fornecida bandeja de suporte para rack 19”. • O software deverá ser fornecido em sua versão mais atualizada. • Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:		

			• Deve suportar os seguintes tipos de NAT. ✓ NAT dinâmico (Many-to-1). ✓ NAT estático (1-to-1). ✓ NAT estático bidirecional 1-to-1. ✓ Tradução de porta (PAT). ✓ NAT de Origem. ✓ NAT de Destino. ✓ Suportar NAT de Origem e NAT de Destino simultaneamente. ✓ Enviar log para sistemas de monitoração externos, simultaneamente. • Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL ou OPSEC. • Proteção contra anti-spoofing. • Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPFv2 ou v3). • Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv2 ou v3). • Deve vir acompanhado de licença para ingresso em console centralizada. **Controle por Política de Firewall, atendendo aos seguintes requisitos mínimos:** • Controles de políticas por porta e protocolo. • Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações. • Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança ou grupos de objetos. • Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound). • Suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound) ou permitir a inserção de certificado no gateway. • Deverá de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2. • Controle de inspeção e de-criptografia por política.		

			• Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg. • Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo). • QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações. • Suporte a objetos e regras IPV6. • Suporte a objetos e regras multicast. • Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente. **Controle de Aplicações, atendendo aos seguintes requisitos mínimos:** • Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades: • Deverá ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos. • Reconhecer pelo menos 1300 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. • skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc. • Inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389.		

			• Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443. • 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, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas. • Identificar o uso de táticas evasivas via comunicações criptografadas. • Atualizar a base de assinaturas de aplicações automaticamente. • Reconhecer aplicações em IPv6. • Limitar a banda (download/upload) usada por aplicações, (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD. • Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory. • Deverá ser possível adicionar controle de aplicações em regras de segurança do dispositivo. • Suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos. • O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações. • Alertar o administrador quando uma aplicação for bloqueada. • Possibilitar que o controle de portas seja aplicado para todas as aplicações de firewall.		

			• Alertar o administrador quando uma aplicação for bloqueada. • Possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos. • Possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos. • Possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos. • Possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos. • Deverá ser possível a criação de grupos de aplicações. **Prevenção de Ameaças, atendendo aos seguintes requisitos mínimos:** • 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 ou entregue através de composição com outro equipamento. • Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware). • As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo determinado enquanto existir contrato de software com fabricante. • Sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo. • Quando utilizada as funções de IPS, Antivírus e Anti-spyware, o equipamento deve garantir performance suficiente para que todos os recursos estejam disponíveis. Mesmo entre ter 1 única assinatura de IPS habilitada ou ter todas as assinaturas de IPS, Anti-Virus e Antispyware habilitadas simultaneamente.		

			• As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração. • Suportar políticas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes políticas, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens. • Permitir o bloqueio de vulnerabilidades. • Permitir o bloqueio de exploits conhecidos. • Incluir proteção contra-ataques de negação de serviços. • Possuir os seguintes mecanismos de inspeção de IPS: • Análise de padrões de estado de conexões. • Análise para detecção de anomalias de protocolo. • Análise heurística. • Bloqueio de pacotes malformados. • Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc. • Detectar e bloquear portscans ou bloquear através de regra de firewall. • Bloquear ataques efetuados por worms conhecidos. • Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS, tratadas por IPS. • Possuir assinaturas para bloqueio de ataques de buffer overflow. • Permitir o bloqueio de vírus e spywares em protocolos HTTP, FTP, SMTP e POP3. • Suportar bloqueio de arquivos por tipo. • Identificar e bloquear comunicação com botnets. • Suportar várias técnicas de prevenção (Drop). • Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: ✓ O nome da assinatura ou do ataque. ✓ Aplicação. ✓ Usuário. ✓ Origem. ✓ Destino. ✓ Ação tomada pelo dispositivo.		

			• Possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos. • Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMTP e POP3. • Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms. • Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos. • Rastreamento de vírus em pdf. • Permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.) • 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, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, grupo de objetos. **Filtro de URL, atendendo aos seguintes requisitos mínimos:** • Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, dia da semana e hora). • Deverá ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança ou grupo de objetos. • Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local. De modo que o firewall possa utilizar das informações para realizar autenticações. • Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.		

			• Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL. • Bloquear o acesso a sites de busca de acordo com uma categoria pré-definida já nativa para a solução. • Suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs. • Possuir pelo menos 56 categorias de URLs. • Suportar a criação categorias de URLs customizadas. • Suportar a exclusão de URLs do bloqueio, por categoria. • Permitir a customização de página de bloqueio. • Suportar a inclusão nos logs do produto de informações sobre qual usuário acessou um determinado site, com a possibilidade de filtro por usuário. **Identificação de Usuários, atendendo aos seguintes requisitos mínimos:** • 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. • Possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários. • Possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários. • Possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários. • A integração com o Microsoft Active Directory poderá ser feita com ou sem a instalação de aplicação cliente no servidor Controlador de Domínio. • Não serão aceitos qualquer tipo de software, aplicação ou agente a ser instalado nos computadores clientes		

			para autenticação do Microsoft Active Directory, LDAP ou qualquer outra funcionalidade do Firewall que não seja a de VPN. • 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). **QoS, atendendo aos seguintes requisitos mínimos:** • Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controla-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming. • Suportar a criação de políticas de QoS por: • Endereço de origem. • Endereço de destino. • Por usuário e grupo do LDAP/AD. • Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus. • Por porta. • O QoS deve possibilitar a definição de classes por: ✓ Banda Garantida. ✓ Banda Máxima. ✓ Fila de Prioridade. • Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP. • Suportar marcação de pacotes Diffserv, inclusive por aplicação. • Disponibilizar estatísticas RealTime para classes de QoS. • Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário. **VPN, atendendo aos seguintes requisitos mínimos:** • 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, 192 e 256 (Advanced Encryption Standard). ✓ Autenticação via certificado IKE PKI. • A VPN SSL deve suportar: ✓ Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB. ✓ A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente. ✓ Atribuição de endereço IP nos clientes remotos de VPN. ✓ Atribuição de DNS nos clientes remotos de VPN. ✓ Permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL. ✓ A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE. • Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local. • Permitir estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon. • Suportar leitura e verificação de CRL (certificate revocation list). • Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL. • O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de		

			maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN. • O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário. • Permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas: • Sob demanda do usuário. • Manter uma conexão segura com o portal durante a sessão. • O agente de VPN SSL client-to-site deve ser compatível com pelo menos: • Windows 7, Windows 8, Windows 8.1 e Windows 10 assim como suas versões subsequentes. • O cliente de VPN SSL cliente-to-site também deve suportar dispositivos móveis (IOS e ANDROID). • Possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna. **Garantia, Suporte, Atualizações e Licenciamento** ✓ Deve ser total, pelo prazo de 3 (três) anos, isentando a Contratante de qualquer ônus decorrente de falhas de hardware ou software durante o período contratado, salvo condições de uso e manipulação indevidas por parte da Contratante. ✓ Deve disponibilizar atualizações de software durante o período mínimo de 3 (três) anos. ✓ Deve disponibilizar atualizações dos sistemas operacionais nativos das soluções durante o período mínimo de 3 (três) anos. ✓ Deve oferecer as seguintes modalidades de suporte, durante o período mínimo de 3 (três) anos. ✓ Suporte e atendimento telefônico em português ou inglês. ✓ Suporte e atendimento via chat em português ou inglês. ✓ Suporte e atendimento remoto. ✓ Deve possuir licenciamento para todos os recursos de software descritos neste Termo de Referência de no mínimo 3 (três) anos.		

			✓ A garantia deverá ser ofertada pela CONTRATADA por meio de recursos próprios ou através de assistência técnica do Fabricante. **Hardware** • Deverá possuir disco SSD ou memória flash com tamanho suficiente para suportar o Sistema Operacional, é obrigatório que o S.O funcione no armazenamento Flash ou SSD. • Deverá possuir um HD de no mínimo 100 GB para armazenamento de logs e demais armazenamentos. • Não será aceito que o Sistema operacional opere em um disco que não seja Flash ou SSD. **Padrões e Certificados de produto** • Deve possuir uma das seguintes certificações: ICSA para Firewall, NSSLabs, Common Criteria ou certificação compatível desde que comprovada a sua compatibilidade. **Balanceamento de links** • Deve possuir o recurso de Failover e balanceamento de uplink. • Deve realizar o balanceamento de no mínimo 4 links através das interfaces Wan. • Deve permitir utilização de Failover e Balance de até 4 interfaces Wan. (SPS 1252)		
VALOR ESTIMADO TOTAL					**R$ 114.400,39**

ANEXO II – FORMULÁRIO DE PROPOSTA DE PREÇOS

LICITANTE: CONTATO:			
END. COMERCIAL: CIDADE:		UF:	CEP:
FONE:	FAX:	E-MAIL:	
CNPJ:		INSCRIÇÃO ESTADUAL:	
DATA: VALIDADE DA PROPOSTA: DADOS BANCÁRIOS (CONFORME ITEM 7.7.): DADOS DO REPRESENTANTE DA EMPRESA (CONFORME ITEM 7.7.):			

ITEM	UN.	QTD	PRODUTO	MARCA	VALOR UNITÁRIO	VALOR TOTAL
01	UN.	01	**FIREWALL** **Especificações técnicas mínimas:** **Especificação Geral:** • Aquisição de solução de proteção de rede para segurança de informação perimetral, firewall, que inclua filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares, Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta. • Por plataforma de segurança entende-se hardware e software integrados do tipo appliance. **Capacidade, atendendo aos seguintes requisitos mínimos:** • A plataforma de segurança deverá possuir a capacidade e as características abaixo: • Funcionalidade de Firewall com throughput de no mínimo 12 GBps.			

			• Appliance deve suportar throughput de no mínimo 2 GBps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS, antivírus e antispyware. • Suportar no mínimo, 4.000.000 de conexões simultâneas. • Suportar no mínimo, 65.000 novas conexões por segundo. • Suportar no mínimo 2000 usuários simultâneos com todas as características do item 2.1.2 habilitadas. • Fonte 120/240 AC. • 06 (seis) interfaces de rede 10/100/1000 base-TX. • 1 (uma) interface do tipo console ou similar para configuração e manutenção. • Deve suportar e estar licenciada para uso de no mínimo 50 (cinquenta) clientes de VPN SSL simultâneos. • Deve suportar o thoughput de 2 Gbps de VPN e 2 Gbps de IPS. • Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento. • A console de gerência e monitoração local pode residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função. **Características Gerais:** • O equipamento deverá ser novo e estar em linha de produção na data do edital. Não serão aceitos equipamentos que já tenham anuncio de fim de vida.			

			• A solução deve consistir de appliance de proteção de rede com funcionalidades de UTM ou NGFW e console de gerência e monitoração. • Por funcionalidade de segurança entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões. • O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. • Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. • O equipamento fornecido deve ser próprio para montagem em rack 19” acompanhado dos kits de instalação ou deverá ser fornecida bandeja de suporte para rack 19”. • O software deverá ser fornecido em sua versão mais atualizada. • Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades: • Deve suportar os seguintes tipos de NAT. ✓ NAT dinâmico (Many-to-1). ✓ NAT estático (1-to-1). ✓ NAT estático bidirecional 1-to-1. ✓ Tradução de porta (PAT). ✓ NAT de Origem. ✓ NAT de Destino. ✓ Suportar NAT de Origem e NAT de Destino simultaneamente. ✓ Enviar log para sistemas de monitoração externos, simultaneamente. • Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL ou OPSEC. • Proteção contra anti-spoofing. • Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPFv2 ou v3).			

			• Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv2 ou v3). • Deve vir acompanhado de licença para ingresso em console centralizada. **Controle por Política de Firewall, atendendo aos seguintes requisitos mínimos:** • Controles de políticas por porta e protocolo. • Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações. • Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança ou grupos de objetos. • Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound). • Suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound) ou permitir a inserção de certificado no gateway. • Deverá de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2. • Controle de inspeção e de-criptografia por política. • Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg. • Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo). • QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações. • Suporte a objetos e regras IPV6. • Suporte a objetos e regras multicast. • Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar			

			políticas em horários pré-definidos automaticamente. **Controle de Aplicações, atendendo aos seguintes requisitos mínimos:** • Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades: • Deverá ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos. • Reconhecer pelo menos 1300 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. • skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc. • Inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389. • Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.			

			• 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, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas. • Identificar o uso de táticas evasivas via comunicações criptografadas. • Atualizar a base de assinaturas de aplicações automaticamente. • Reconhecer aplicações em IPv6. • Limitar a banda (download/upload) usada por aplicações, (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD. • Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory. • Deverá ser possível adicionar controle de aplicações em regras de segurança do dispositivo. • Suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos. • O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações. • Alertar o administrador quando uma aplicação for bloqueada. • Possibilitar que o controle de portas seja aplicado para todas as aplicações de firewall.			

			• Alertar o administrador quando uma aplicação for bloqueada. • Possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos. • Possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos. • Possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos. • Possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos. • Deverá ser possível a criação de grupos de aplicações. **Prevenção de Ameaças, atendendo aos seguintes requisitos mínimos:** • 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 ou entregue através de composição com outro equipamento. • Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware). • As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo determinado enquanto existir contrato de software com fabricante. • Sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo. • Quando utilizada as funções de IPS, Antivírus e Anti-spyware, o equipamento deve garantir			

			performance suficiente para que todos os recursos estejam disponíveis. Mesmo entre ter 1 única assinatura de IPS habilitada ou ter todas as assinaturas de IPS, Anti-Virus e Antispyware habilitadas simultaneamente. • As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração. • Suportar políticas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes políticas, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens. • Permitir o bloqueio de vulnerabilidades. • Permitir o bloqueio de exploits conhecidos. • Incluir proteção contra-ataques de negação de serviços. • Possuir os seguintes mecanismos de inspeção de IPS: • Análise de padrões de estado de conexões. • Análise para detecção de anomalias de protocolo. • Análise heurística. • Bloqueio de pacotes malformados. • Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc. • Detectar e bloquear portscans ou bloquear através de regra de firewall. • Bloquear ataques efetuados por worms conhecidos. • Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS, tratadas por IPS. • Possuir assinaturas para bloqueio de ataques de buffer overflow. • Permitir o bloqueio de vírus e spywares em protocolos HTTP, FTP, SMTP e POP3. • Suportar bloqueio de arquivos por tipo. • Identificar e bloquear comunicação com botnets.			

			• Suportar várias técnicas de prevenção (Drop). • Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: ✓ O nome da assinatura ou do ataque. ✓ Aplicação. ✓ Usuário. ✓ Origem. ✓ Destino. ✓ Ação tomada pelo dispositivo. • Possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos. • Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMTP e POP3. • Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms. • Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos. • Rastreamento de vírus em pdf. • Permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.) • 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, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, grupo de objetos. **Filtro de URL, atendendo aos seguintes requisitos mínimos:** • Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, dia da semana e hora).			

			• Deverá ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança ou grupo de objetos. • Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local. De modo que o firewall possa utilizar das informações para realizar autenticações. • Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório. • Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL. • Bloquear o acesso a sites de busca de acordo com uma categoria pré-definida já nativa para a solução. • Suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs. • Possuir pelo menos 56 categorias de URLs. • Suportar a criação categorias de URLs customizadas. • Suportar a exclusão de URLs do bloqueio, por categoria. • Permitir a customização de página de bloqueio. • Suportar a inclusão nos logs do produto de informações sobre qual usuário acessou um determinado site, com a possibilidade de filtro por usuário. **Identificação de Usuários, atendendo aos seguintes requisitos mínimos:** • 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. • Possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários. • Possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários. • Possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários. • A integração com o Microsoft Active Directory poderá ser feita com ou sem a instalação de aplicação cliente no servidor Controlador de Domínio. • Não serão aceitos qualquer tipo de software, aplicação ou agente a ser instalado nos computadores clientes para autenticação do Microsoft Active Directory, LDAP ou qualquer outra funcionalidade do Firewall que não seja a de VPN. • 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). **QoS, atendendo aos seguintes requisitos mínimos:** • Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controla-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes			

			usuários ou aplicações, tanto de áudio como de vídeo streaming. • Suportar a criação de políticas de QoS por: • Endereço de origem. • Endereço de destino. • Por usuário e grupo do LDAP/AD. • Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus. • Por porta. • O QoS deve possibilitar a definição de classes por: ✓ Banda Garantida. ✓ Banda Máxima. ✓ Fila de Prioridade. • Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP. • Suportar marcação de pacotes Diffserv, inclusive por aplicação. • Disponibilizar estatísticas RealTime para classes de QoS. • Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário. **VPN, atendendo aos seguintes requisitos mínimos:** • 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, 192 e 256 (Advanced Encryption Standard). ✓ Autenticação via certificado IKE PKI. • A VPN SSL deve suportar:			

			✓ Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB. ✓ A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente. ✓ Atribuição de endereço IP nos clientes remotos de VPN. ✓ Atribuição de DNS nos clientes remotos de VPN. ✓ Permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL. ✓ A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE. • Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local. • Permitir estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon. • Suportar leitura e verificação de CRL (certificate revocation list). • Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL. • O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN. • O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário. • Permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas: • Sob demanda do usuário.			

			• Manter uma conexão segura com o portal durante a sessão. • O agente de VPN SSL client-to-site deve ser compatível com pelo menos: • Windows 7, Windows 8, Windows 8.1 e Windows 10 assim como suas versões subsequentes. • O cliente de VPN SSL cliente-to-site também deve suportar dispositivos móveis (IOS e ANDROID). • Possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna. **Garantia, Suporte, Atualizações e Licenciamento** ✓ Deve ser total, pelo prazo de 3 (três) anos, isentando a Contratante de qualquer ônus decorrente de falhas de hardware ou software durante o período contratado, salvo condições de uso e manipulação indevidas por parte da Contratante. ✓ Deve disponibilizar atualizações de software durante o período mínimo de 3 (três) anos. ✓ Deve disponibilizar atualizações dos sistemas operacionais nativos das soluções durante o período mínimo de 3 (três) anos. ✓ Deve oferecer as seguintes modalidades de suporte, durante o período mínimo de 3 (três) anos. ✓ Suporte e atendimento telefônico em português ou inglês. ✓ Suporte e atendimento via chat em português ou inglês. ✓ Suporte e atendimento remoto. ✓ Deve possuir licenciamento para todos os recursos de software descritos neste Termo de Referência de no mínimo 3 (três) anos. ✓ A garantia deverá ser ofertada pela CONTRATADA por meio de recursos próprios ou através de assistência técnica do Fabricante.			

			Hardware • Deverá possuir disco SSD ou memória flash com tamanho suficiente para suportar o Sistema Operacional, é obrigatório que o S.O funcione no armazenamento Flash ou SSD. • Deverá possuir um HD de no mínimo 100 GB para armazenamento de logs e demais armazenamentos. • Não será aceito que o Sistema operacional opere em um disco que não seja Flash ou SSD. **Padrões e Certificados de produto** • Deve possuir uma das seguintes certificações: ICSA para Firewall, NSSLabs, Common Criteria ou certificação compatível desde que comprovada a sua compatibilidade. **Balanceamento de links** • Deve possuir o recurso de Failover e balanceamento de uplink. • Deve realizar o balanceamento de no mínimo 4 links através das interfaces Wan. • Deve permitir utilização de Failover e Balance de até 4 interfaces Wan. (SPS 1252)			
					VALOR TOTAL	**R$**

ANEXO III – CRONOGRAMA DE DESEMBOLSO FINANCEIRO

CRONOGRAMA DE DESEMBOLSO FINANCEIRO											
Objeto: Aquisição de solução de segurança firewall para a proteção da rede corporativa do Sistema Fibra visando atender demanda da Gerência de Informática.											
DESCRIÇÃO DOS CUSTOS	**QTDE**	**UNIDADE**	**DIAS**								
			20	**25**	**30**	**35**	**40**	**45**	**50**	**55**	**60**
Aquisição de solução de segurança firewall para proteção de rede corporativa do Sistema Fibra.	1	UND			R$ 114.400,39						
Valor Total (R$)					**R$ 114.400,39**						

ANEXO IV – DECLARAÇÃO DE QUE NÃO EMPREGA MENOR

A empresa.....(Razão Social), inscrita no CNPJ sob o n° (MATRIZ) ....., por intermédio de seu representante legal o(a) Sr(a)..... portador(a) da Carteira de Identidade - RG nº..... e do CPF nº.....DECLARA, sob as penas da lei, para fins do disposto no inciso V, art. 27, da Lei federal n° 8.666/93, em cumprindo ao inciso XXXIII, art. 7º, da Constituição Federal, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos, assim como assume o compromisso de declarar a superveniência de qualquer fato impeditivo à sua habilitação.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ( )

Em,.....de.....de 20....

.....
(assinatura do representante legal)

(Observação: em caso afirmativo, assinalar a ressalva acima)

ANEXO V –DECLARAÇÃO DE GARANTIA DO EQUIPAMENTO.

Declaro(amos) sob as penas da lei, que a (nome da pessoa jurídica) assume o compromisso da garantia mínima de 12 (doze) meses para os equipamentos ofertados no **Pregão Eletrônico nº 39/2016,** do SERVIÇO SOCIAL DA INDÚSTRIA – SESI/DF, contra defeitos de fabricação, a partir da data de emissão da nota fiscal.

Em,.....de.....de 2016.

_____

(Nome completo do representante legal da licitante)

_____

(Nº da CI do representante legal da licitante)

_____

(Assinatura do representante legal da licitante)