I – EDITAL SESI SENAI/DF Nº: 08/2016

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

III – MODALIDADE: PREGÃO ELETRÔNICO

IV – PROCESSO Nº: 015.792/2016

V – TIPO: MENOR PREÇO POR ITEM

VI – FORMA DE FORNECIMENTO: CONFORME DEMANDA DO SESI E SENAI - CIF/BRASÍLIA-DF

VII – RECEBIMENTO DAS PROPOSTAS E LANCES:

INÍCIO DO RECEBIMENTO DAS PROPOSTAS: 22 de novembro de 2016.

ENCERRAMENTO DAS PROPOSTAS: 02 de dezembro de 2016. (ANTES DA ABERTURA DA SESSÃO DE LANCES).

ABERTURA DA SESSÃO DE LANCES: 02 de dezembro de 2016 às 09h30min (Horário de Brasília)

COMPROVANTE DE ENTREGA DO EDITAL

Recebi do SERVIÇO SOCIAL DA INDÚSTRIA – SESI/DR-DF e SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI/DR-DF – Departamentos Regionais do Distrito Federal, o Edital de **PREGÃO ELETRÔNICO Nº 08/2016,** tipo **MENOR PREÇO POR ITEM,** cuja realização (abertura da sessão de lances) dar-se-á às **09h30min (Horário de Brasília)**, do dia **02 de dezembro 2016**, no sítio eletrônico www.pregao.com.br .

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

RAZÃO SOCIAL: _____

ENDEREÇO: _____

CNPJ: _____ TEL: _____ FAX: _____

RESPONSÁVEL: _____

CPF:_____ E-MAIL: _____

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 e Serviço Nacional de Aprendizagem Industrial - SENAI/DF – Departamentos Regionais do Distrito Federal, por meio do **e-mail compras@sistemafibra.org.br.**

SERVIÇO SOCIAL DA INDÚSTRIA – SESI/DR-DF e SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL SENAI/DR-DF – Departamentos Regionais do Distrito Federal comunicarão as licitantes cadastradas eventuais retificações ocorridas no instrumento convocatório, bem como de quaisquer informações adicionais, no sítio eletrônico: www.pregao.com.br; ou via fax ou por meio de correspondência eletrônica.

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

I – EDITAL SESI SENAI/DF Nº: 08/2016

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

III - MODALIDADE: PREGÃO ELETRÔNICO

IV - PROCESSO Nº: 015.792/2016

V - TIPO: MENOR PREÇO POR ITEM

VI – FORMA DE FORNECIMENTO: CONFORME DEMANDA DO SESI E SENAI - CIF/BRASÍLIA-DF

VII – RECEBIMENTO DAS PROPOSTAS E LANCES:

INÍCIO DO RECEBIMENTO DAS PROPOSTAS: 22 de novembro de 2016.

ENCERRAMENTO DAS PROPOSTAS: 02 de dezembro de 2016. (ANTES DA ABERTURA DA SESSÃO DE LANCES).

ABERTURA DA SESSÃO DE LANCES: 02 de dezembro de 2016 às 09h30min (Horário de Brasília)

1. DA CONVOCAÇÃO

1.1. SERVIÇO SOCIAL DA INDÚSTRIA – SESI/DR-DF e SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI/DR-DF – Departamentos Regionais do Distrito Federal, com sede no SIA Trecho 3, 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, SESI/SENAI-DF Nº 08/2016**, às **09h30min (horário de Brasília)**, do **dia 02 de dezembro de 2016**, na forma estabelecida neste Edital SESI/SENAI-DFe de acordo com o disposto no Regulamento de Licitações e Contratos do SESI SENAI, 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 software antivírus para a proteção da rede corporativa do SESI SENAI, visando atender demanda da Gerência de Tecnologia da Informação do SESI SENAI/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 sítio eletrônico: www.pregao.com.br, ou na Coordenação de Aquisição, localizada no seguinte endereço: SIA Trecho 3, Lote 225, Edifício FIBRA, Subsolo, 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 data de assinatura da Autorização de Prestação de Serviços - APS.

3.2. **Do Local de Entrega:** Gerência de Tecnologia da Informação do SESI SENAI**,** Endereço**:** SIA Trecho 3, Lote 225 Edifício FIBRA Brasília – DF CEP: 71200-030 –Tel (061) 3362 6000.

4. DA PARTICIPAÇÃO

4.1. Somente poderão participar deste Pregão Eletrônico as empresas legalmente estabelecidas no território nacional, de ramo compatível ao 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, por meio 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. Que 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/SENAI-DFsuspenso ou que por esta entidade tenham sido declaradas inidôneas.

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

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

4.3.1. Empregado, dirigente ou Conselheiro do SESI/SENAI-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/SENAI-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/SENAI-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/SENAI-DF Nº 08/2016**.

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 2 (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, de modo que os valores informados sejam idênticos.

7.3.1 A proposta de preços constante no Anexo II, deverá conter preço unitário e total para cada 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 total da proposta expresso em algarismo e por extenso.

7.4. Deverá constar na proposta de preços a marca dos 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 (três) 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 neste Edital e seus Anexos.

7.8. A licitante vencedora fica obrigada a garantir a qualidade do software ofertado, obrigando-se a substituir, imediatamente, caso esteja fora do padrão, sem quaisquer ônus para este SESI/SENAI-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. O 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 instrumento, 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 localizada no SIA Trecho 3, Lote 225, Edifício FIBRA – Brasília/DF, CEP: 71.200-030. No verso do envelope que irá conter este documento, deve-se fazer referência ao número do Edital PREGÃO ELETRÔNICO SESI/SENAI-DF Nº 08/2016.

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

8. DA DIVULGAÇÃO DAS PROPOSTAS DE PREÇOS

8.1. A partir das **09h30min** do **dia 02 de dezembro de 2016** e em conformidade com o Item 5 deste Edital, será aberta a sessão pública do Pregão Eletrônico **SESI/SENAI-DF Nº 08/2016**, com a divulgação pela Pregoeira por meio 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/SENAI-DFestá disposto a pagar pelo objeto da licitação.

9.2. A apresentação de proposta com valor acima do estimado pelo SESI/SENAI-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/SENAI-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 para estes.

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 do 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/SENAI-DF Nº 08/2016**, 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, 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/SENAI-DF Nº 08/2016.

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 as 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.

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

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 da 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 junto ao Instituto Nacional de Seguridade Social – CND/INSS, dentro do prazo de validade.

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

e.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.

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

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

12.1.3. 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 12.440/2011, dentro do prazo de validade.

12.1.4. Quanto à Qualificação Técnica:

a) Apresentação de atestado(s) ou certidão(ões) de capacidade técnica, fornecido(s) por pessoa(s) jurídica(s), de direito público ou privado, no(s) qual(is) deverá(ão) estar comprovado(s) que a empresa participante fornece ou forneceu satisfatoriamente itens compatíveis com o objeto desta licitação, podendo ser exigido da licitante vencedora, apresentação da cópia autenticada do Contrato da prestação de serviço ou da nota fiscal que deram origem ao atestado.

a.1) A comprovação a que se refere a alínea acima dar-se-á 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 que forneceu o material ao emitente.

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-DFpoderá exigir da proposta melhor classificada à apresentação de cópia autenticada da Nota Fical ou Instrumento Contratual que deram origem ao Atestado.

12.1.5. Quanto à Qualificação Econômica-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.

12.1.6. 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 sites 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 descrição: Serviço Social da Indústria - Departamento Regional do Distrito Federal – **Pregão Eletrônico SESI/SENAI-DF Nº 08/2016**.

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 na 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.

14. DOS RECURSOS ADMINISTRATIVOS

14.1. 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.

14.2. A decisão da Pregoeira sobre o recurso deverá ser motivada e submetida à apreciação da autoridade responsável pela licitação.

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

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

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

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

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

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

15. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

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

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

16 - DA ASSINATURA DA AUTORIZAÇÃO DE SERVIÇOS - APS

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

16.2. Independentemente de sua transcrição, para todos os efeitos legais, farão parte da Autorização de Serviços que vier a ser assinada todas as condições estabelecidas no presente Edital e seus Anexos, na Proposta de Preços e na Documentação de Habilitação, apresentadas pela licitante vencedora.

16.3. 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 da Autorização de Serviços – APS atualizado, conforme Artigo 30 do Regulamento de Licitações e Contratos do SESI SENAI.

16.4. A licitante vencedora deverá comparecer à Coordenação de Aquisição do SESI/DF, no prazo máximo de **5 (cinco) dias úteis**, contados de sua convocação para assinatura da Autorização de Serviços - APS.

16.5. A vigência deste instrumento contratual será de **03 (três) meses,** contados da data de sua assinatura.

17. DAS OBRIGAÇÕES DA CONTRATADA

17.1. 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 SENAI, que o regem:

17.1.1. Vedar a veiculação, publicidade ou quaisquer informações acerca das atividades objeto deste Edital, sem a prévia e expressa autorização do SESI/DF e SENAI/DF.

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

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

17.1.4. Emitir nota fiscal dos antivírus fornecidos, ficando vedada a inclusão de item adverso ao contratado na mesma nota fiscal.

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

17.1.6. Responsabilizar-se por todas as despesas em caso de devolução dos antivírus por estarem em desacordo com as especificações técnicas descritas neste Edital.

17.1.7. Assumir o compromisso de indenizar o SESI/SENAI-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.

17.1.8. Executar fielmente o fornecimento nas especificações e prazos, não se admitindo modificações sem prévia consulta e concordância do SESI/DF e SENAI/DF.

17.1.9. Responsabilizar-se integralmente pelo fornecimento contratado, nos termos da legislação vigente.

17.1.10. Não transferir a outrem, no todo ou em parte, o Instrumento Contratual, sem prévia e expressa anuência do SESI/DF e SENAI/DF.

17.1.11. Dispor de quadro de pessoal suficiente para o atendimento do fornecimento sem interrupção, seja por motivo de férias, descanso semanal, licença, falta ao serviço, demissão e outros análogos.

17.1.12. Participar das reuniões com o SESI/DF e SENAI/DF sempre que solicitada.

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

18. DAS OBRIGAÇÕES DO SESI/SENAI-DF

18.1. 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, desde que respeitadas às condições e quantidades pactuados.

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

18.3. 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.

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

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

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

18.7. Atestar a Nota Fiscal relativa à aquisição do software antivírus em conformidade com o estabelecido neste Edital, por meio do setor competente.

18.8. Esclarecer eventuais dúvidas sobre detalhes da aquisição do software antivírus e possíveis interferências que porventura não tenham sido suficientemente esclarecidas ou previstas.

19. DA FORMA DE PAGAMENTO

19.1. A empresa CONTRATADA apresentará Nota Fiscal/Fatura, conforme demanda do SESI/SENAI-DF, para liquidação e pagamento da despesa, em 2 (duas) vias, acompanhadas da documentação constante do subitem 12.1.2: letra “a” (**CNPJ**), letra “c” (**FGTS**), letra “d” (**INSS**), letra “e.1” (**CERTIDÃO DE TRIBUTOS FEDERAIS**), letra “e.2” (**PROVA DE REGULARIDADE COM O GDF)** e “e.3” **(PROVA DE REGULARIDADE COM A FAZENDA ESTADUAL E/OU MUNICIPAL)** para as empresas sediadas em outras localidades. A empresa contratada estará sujeita às retenções tributárias legais, devendo a mesma informar no corpo da Nota Fiscal às deduções as quais ela se adequa.

19.2. O pagamento será efetuado, em parcela única, por meio de depósito em conta bancária, em nome da Contratada, em até **30 (trinta) dias**, após o recebimento e aceite da(s) nota(s) fiscal(is).

19.3. As Notas Fiscais/Faturas para liquidação e pagamento da despesa deverão estar, obrigatoriamente, atestadas pelo setor competente, bem como acompanhada da documentação constante do subitem 19.1, dentro do prazo de validade.

19.4. Para liquidação dos valores relativos à entrega do software antivírus do objeto será ainda observado o que segue:

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

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

19.4.3. As Notas Fiscais não aprovadas pelo SESI/SENAI-DF serão devolvidas à empresa Contratada para as devidas correções, acompanhadas dos motivos de sua rejeição, recontando-se para pagamento o prazo estabelecido no subitem 19.2, a partir da sua reapresentação, sem qualquer tipo de correção de seu valor, sendo automaticamente alterada a data de vencimento, não respondendo a Contratante por quaisquer encargos resultantes de atrasos na liquidação do pagamento correspondentes.

20 - DAS PENALIDADES

20.1. Salvo hipótese de caso fortuito ou de força maior, a inexecução total ou parcial injustificada, a execução deficiente, irregular ou inadequada do objeto deste Edital, assim como o descumprimento dos prazos e condições estipulados, implicará a aplicação das penalidades abaixo explicitadas, aplicadas isolada ou cumulativamente, com determinação e grau de aplicação a critério do SESI/SENAI-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.

20.2. Caso a licitante vencedora não aceitar, receber e assinar o Instrumento Contratual, dentro do prazo máximo previsto, no subitem 16.3, este deverá ser anulado, sujeitando-se a licitante faltosa à multa de 10% (dez por cento) calculado sobre o valor considerado em sua proposta.

20.3. No caso de aplicação de qualquer das multas previstas nos subitens anteriores, estas serão descontadas de qualquer fatura ou crédito existente em favor da licitante Contratada.

20.4. 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 2 (dois) anos.

20.5. Para aplicação das penalidades aqui previstas, a empresa Contratada será notificada para apresentar defesa prévia no prazo máximo de 5 (cinco) dias úteis, contados da sua notificação.

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

25. DAS DISPOSIÇÕES GERAIS

25.1. O SESI/SENAI-DF não admitirá, após recebimento dos envelopes de “PROPOSTA DE PREÇOS” e “DOCUMENTAÇÃO DE HABILITAÇÃO”, alegações 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.

25.2. São partes integrantes deste Edital, os seguintes Anexos:

- ANEXO I – PLANILHA DE 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.

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

25.4. Decairá do direito de impugnar os termos deste Edital perante o SESI/SENAI-DF a licitante que não o fizer até **2 (dois) dias úteis anteriores à data de abertura**, quanto a eventuais falhas ou irregularidades no Edital, hipótese em que tal comunicação não terá efeito de recurso.

25.5. Qualquer pedido de esclarecimento sobre este Edital deverá ser encaminhado, por escrito, a Pregoeira, entregue e protocolado no **SIA Trecho 3, 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.**

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

25.7. É facultado ao SESI/SENAI-DF, quando a convocada não assinar o Instrumento Contratual, dentro do prazo que trata nos subitens 16.3, convocar as licitantes remanescentes, observada 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.

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

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

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

Brasília – DF, 22 de novembro de 2016.

Patricia de Castro Machado Gomes
Pregoeira

ANEXO I – PLANILHA DE ESTIMATIVA DE PREÇOS

ITEM	QTDE	UN.	DESCRIÇÃO	PREÇO UNITÁRIO ESTIMADO (R$)	PREÇO TOTAL ESTIMADO (R$)
01	872	UN.	**LICENÇAS DE SOFTWARE ANTIVÍRUS** **Servidor de administração e console administrativa.** **A Console da solução deve possuir as seguintes características:** • A console de gerenciamento deve ser acessível via Web; • A console de gerenciamento central deverá ser compatível com os ambientes de virtualização: Microsoft Hyper V, VMware vSphere, View, VMware Player, Citrix XenServer, XenDe.sktop, VDI-in-a-Box, Red Hat Enterprise Virtualization, Oracle VM, Kernel-basedVirtual Machine or KVM; • A solução deverá ser integrável com Microsoft Active Directory, Citrix XenServer e VMware vCenter, na descoberta e no gerenciamento das máquinas virtualizadas; • Deve permitir a instalação de mais de 1 Virtual Appliance para cada componente de gerenciamento; • Capacidade de criação de mais de um usuário com privilégios administrativos; • Capacidade de criação de usuários com privilégios apenas para visualização de relatórios; • Capacidade de efetuar logon no console de gerenciamento com as credenciais do Active Directory; • Capacidade de descoberta das máquinas por domínio; • Função especial de “relay” ou retransmissores ilimitados (espalhados pela matriz e escritórios	R$ 186,15	R$ 162.322,80

			remotos/localidades/filiais) dos pacotes de instalação com as políticas de segurança além das atualizações locais da base de assinaturas de vírus (definições conhecidas de malwares); • Função especial de varredura central com agente leve para a proteção, varredura e remoção de vírus na memória, trilha zero de boot e arquivos dos servidores e estações físicas ou virtuais; • Deve permitir o gerenciamento centralizado através da mesma console de estações, servidores, laptops, mobile e computadores/servidores virtualizados; • Remover automaticamente qualquer software antivírus que houver instalado no computador (estações e servidores) no momento da instalação do Antivírus; • Mecanismo de Comunicação em tempo real, entre servidor e clientes, para entrega de configurações e assinaturas; • Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo e login script; • Capacidade de gerar pacotes customizados (autoexecutáveis) para instalação local nos computadores; • Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas; • Capacidade de monitorar diferentes subredes a fim de encontrar máquinas novas para serem adicionadas à proteção; • Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para ser adicionadas à proteção; • Capacidade de instalação e atualização do		

			Software sem intervenção do usuário; • Capacidade de agrupamento de máquina por Grupos ou Estrutura do Active Directory; • Capacidade de definir políticas de configurações diferentes pela estrutura do Active Directory e por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos; • Deve fornecer as seguintes informações dos computadores: ➢ Se o antivírus está instalado; ➢ Se o antivírus está iniciado; ➢ Se o antivírus está atualizado; ➢ Tempo de comunicação desde a última conexão da máquina com o servidor administrativo; ➢ Última atualização de vacinas ➢ Última verificação executada na máquina; ➢ Versão do antivírus instalado na máquina; ➢ Necessidade de reiniciar o computador para aplicar mudanças; ➢ Quantidade de vírus encontrados (contador) na máquina; ➢ Nome do computador; • Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las; • Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação (update Server), sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de atualização, a fim de otimizar tráfego da rede; • Capacidade de exportar relatórios para os		

			seguintes tipos de arquivos: PDF e XLS e/ou PDF e CSV • Capacidade de enviar E-mails para contas específicas em caso de algum evento; • Capacidade de realizar atualização incremental de vacinas nos computadores clientes; • Capacidade de reiniciar as máquinas remotamente; • Possuir a Tecnologia de analise comportamental de detecção para vírus e ameaças desconhecidas que analisa o comportamento de códigos potencialmente maliciosos dentro de um ambiente virtual seguro de um computador, eliminando os falsos positivos e aumentando as taxas de detecção de malware desconhecidos. • O fabricante da solução ofertada deverá possuir o prêmio/certificado AV Test e não poderá ter recebido notas inferiores a 4,5 em testes feitos nos últimos 12 meses. • O Fabricante/Desenvolvedor da solução deverá obrigatoriamente ser participante do programa MAPP (Microsoft Active Protections Program), garantindo assim o recebimento antecipado de informações sobre vulnerabilidades e segurança sobre a plataforma Microsoft; **Descrição da Proteção para Servidores e Estações de trabalhos** Compatibilidade: ✓ Microsoft Windows 7 ✓ Microsoft Windows 8 ✓ Microsoft Windows 8.1 ✓ Windows 10 ✓ Windows Server 2008 ✓ Windows Server 2008 R2 ✓ Windows Server 2012		

			✓ Windows Server 2012 R2 **Características:** Deve prover as seguintes proteções: • Proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos; • Proteção antispyware deve ser nativa do próprio antivírus, sem necessidade de plugin ou instalação adicional; • AntiPhising (módulo para verificação e classificação de sites e downloads contra vírus); • Verificação de vírus nas mensagens de correio eletrônico, suportando clientes Outlook; • Permitir o escaneamento das ameaças de maneira manual, agendado ou em tempo real, detectando ameaças no nível do Kernel do Sistema Operacional com capacidade de detecção de rootkits; • Permitir o isolamento de arquivos, para área de quarentena, para serem enviados e vistoriados pelo centro de pesquisa do fabricante; • Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo, reparar, apagar, mover para área de isolamento e ignorar; • Deve possui Firewall que suporte os protocolos TCP, UDP e ICMP no mínimo; • Autoproteção (contra-ataques aos serviços/processos do antivírus); • Controle de execução de aplicativos; • Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota; • As vacinas devem ser atualizadas pelo fabricante e disponibilizadas via servidor		

			central de gerenciamento, podendo ser configurada a base de atualização como primeira atualização, em caso de falha do servidor de atualização principal, as estações devem buscar a atualizações no site do fabricante, sendo possível configurar a hora de atualização nas estações e proxy; • Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução; • Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, removendo a solução no momento da instalação do antivírus; • Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão com o Nome do arquivo para que qualquer objeto detectado escolhido seja ignorado; • Capacidade de verificar arquivos zipados (incluindo .zip, rar); • Capacidade de verificar objetos usando heurística; • O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: ➢ Perguntar o que fazer, ou; ➢ Bloquear acesso ao objeto; ➢ Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador); ➢ Em caso positivo de desinfecção, restaurar o objeto para uso; ➢ Em caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);		

			➢ Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto; • Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3 e SMTP; • Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings; • Capacidade de verificar links inseridos em e-mails contra phishings; • Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox, Safari e Chrome; • Possibilidade de verificar e-mails enviados e recebidos; • Capacidade de filtrar anexos de e-mail, apagando-os de acordo com a configuração feita pelo administrador; • Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas; • Na verificação de tráfego web, caso encontrado código malicioso o programa deve: ➢ Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio; ➢ Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou; ➢ Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação; • Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web; • Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-		

			as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas; • Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa; • Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas; • Deve possuir módulo Firewall para proteção contra exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas; • O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: ➢ Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; ➢ Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo ou nome de aplicativo terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados; ➢ Opção de Criar Perfis de Rede ou Zonas; ➢ Controle de Conexão; ➢ Deve possuir o Modo Invisível onde em caso de tentativa de Port Scan a maquinas parem de responder e fiquem invisível a tentativa de escaneamento; • Capacidade de limitar a execução de aplicativos por nome do arquivo ou hash. (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc.); • Capacidade de, caso o computador cliente saia da rede corporativa, possa atualizar as vacinas via site do fabricante e manter as		

			regras originadas da Console de gerenciamento. • Prover módulo onde o usuário consiga alterar qualquer configuração do antivírus de forma local; • Capacidade de ter escaneamento hibrido, tanto com o servidor que está na internet, quanto via servidor local. Esse servidor local deve ser virtualizado e armazenar grande parte do motor do antivírus para melhorar a performance da estação com poucos recursos disponíveis. • Deve possuir módulo para bloqueio de dispositivos, com no mínimo os seguintes itens: ➢ Bluetooth ➢ CDROM ➢ Drive de disquete ➢ IEEE 1284.4 ➢ IEEE 1394 ➢ Modem ➢ Drives de fita ➢ Portas COM/LPT ➢ Discos SCSI em Raid ➢ Impressoras ➢ Adaptadores de rede ➢ Adaptadores de rede Wireless ➢ Armazenamento interno ➢ Armazenamento externo **Descrição das Estações de Trabalho Linux** Compatibilidade: • Plataforma 32/64bits: • Red Hat Enterprise Linux / CentOS 5.6 ou superior • Ubuntu 11.04 LTS ou superior • OpenSUSE 11 ou superior • Fedora 16 ou superior		

			• Debian 6.0 ou superior **Características:** Deve prover as seguintes proteções: • Antivírus de arquivos (AntiSpyware, AntiTrojan, AntiMalware); • Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: ➢ Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); ➢ Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena; ➢ Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares; ➢ Capacidade de verificar arquivos compactados em até 20 níveis; ➢ Capacidade de verificar arquivos compactados em até 80 tipos de formatos; ➢ Capacidade de verificar objetos usando heurística; • Deve possuir integração com o módulo de administração Central ou através de ferramenta nativa; **Descrição da Proteção para Servidores de E-mails Exchange** Características • Compatibilidade com Servidores Exchange 2007/2010/2013		

			• Deve possuir as seguintes características: • Deve Possuir os Filtros de AntiSpam, Antiphishing, Antispyware e Filtragem de Conteúdo; • Capacidade de verificar todos os e-mails enviados e recebidos contra vírus, Trojan, spyware e qualquer tipo de código malicioso e potencialmente hostil em anexos e no corpo do e-mail; • Capacidade de varrer o sistema de arquivos do servidor sob demanda; • Capacidade de verificar somente objetos novos ou alterados; • Capacidade de filtrar anexos por nome e tipo de arquivo; • Capacidade de filtrar anexos por nome e tipo de arquivo e bloquear o recebimento ou envio do mesmo de acordo com as regras do Administrador; • Capacidade de agrupar usuários e criar regras por grupos; • Capacidade de armazenar cópias de arquivo infectado antes da tentativa de desinfecção; • Capacidade de colocar em quarentena arquivos suspeitos ou danificados; • Possuir Filtro Bayesiano de classificação de Mensagens • Capacidade de enviar notificações de objetos suspeitos e infectados para o administrador, remetente e destinatário da mensagem; • Deve possuir atualização de vacinas automáticas e sob demanda. O fabricante deve submeter novas atualizações com frequência horária, independentemente do nível de ameaça sendo possível configurar o intervalo de agendamento de horários de atualização das Vacinas e Produto;		

			Descrição da Proteção para Mobiles Compatibilidade: • Smartphones e Tablets Android 2.2 ou Superior; • Smartphones e Tablets iOS 5 ou Superior **Características:** Deve prover as seguintes proteções: • Antivírus de arquivos residente (AntiSpyware, AntiTrojan, AntiMalware, antiSpam) que verifique qualquer arquivo criado, acessado ou modificado. As vacinas devem ser atualizadas pelo fabricante; • Capacidade de bloquear a tela do dispositivo com senha; • Capacidade de apagar os dados do dispositivo em caso de perda ou roubo do aparelho; • Capacidade de descobrir a localização do aparelho em caso de perda ou roubo; • Capacidade de escaneamento em tempo real e criptografia para dispositivos Android; • Capacidade de gerenciamento integrado com Microsoft Active Directory; **Descrição da Proteção para Servidores e Estações de trabalho virtualizados** • Plataforma de virtualização suportada: • VMware vSphere 6, VMware vSphere 5.1, 5.0, 4.1 com VMware vCenter Server 6.0, 5.1, 5.0, 4.1 • VMware View 5.1, 5.0 • Microsoft Hyper-V Server 2008 R2 • Microsoft Hyper-V Server 2012 • Microsoft Hyper-V Server 2012 R2 **Sistemas operacionais suportados para proteção em virtualização:** • Fedora 16, 15 • SUSE Linux Enterprise Server 11 • Ubuntu 12.04		

			• Red Hat Enterprise Linux / CentOS 6.2, 6.1, 5.7, 5.6 • Windows Vista • Windows 7 • Windows 8 • Windows Server 2003 • Windows Server 2003 R2 • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 **Características:** Deve prover as seguintes proteções: • Capacidade de proteger máquinas virtuais através da integração com VMware vShield Endpoint sem necessidade de instalação de agentes; • Capacidade de fazer o escaneamento nas máquinas virtuais através da integração com VMware Vshield Endpoint instalados mesmo com a máquina virtual off-line; • Capacidade de proteger ambiente virtualizado em qualquer plataforma de virtualização instalada; • Capacidade de proteger arquivos de sistema, processos e memória em Windows e Linux; • Capacidade de realizar escaneamento das máquinas que estão desligadas (escaneamento off-line); • Antivírus de Arquivos residente (antispyware, antitrojan, antimalware, etc.) que verifique qualquer arquivo criado, acessado ou modificado; • As vacinas devem ser atualizadas pelo fabricante; • Capacidade de verificar arquivos compactados com a opção de colocar quantos níveis de		

			compactação deve ser o escaneamento; • Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.); • Capacidade de verificar objetos usando heurística; • Capacidade de configurar diferentes ações para diferentes tipos de ameaças; • Caso o Servidor seja File Server, instalar além do agente o Módulo de File Server onde deverá mostrar as seguintes informações por dia, semana ou mês: **a)** Itens analisados, Itens infectados, Itens suspeitos, Itens limpos, Itens não analisados, vírus individuais, Riskware individual, spyware, adware, aplicações, discadores, Itens resolvidos, desinfectado, apagado, movido para quarentena, acesso bloqueado, ignorado; Capacidade de atualizar o módulo de proteção sem reiniciar o servidor. **Suporte, Manutenção e Licenciamento** ✓ **Garantia:** pelo prazo de 3 (três) anos, contados a partir da data da entrega do software, isentando o SESI/SENAI de qualquer ônus decorrente de falhas do software durante o período contratado, salvo condições de uso e manipulação indevidas por parte do SESI/SENAI. ✓ **Atualizações de software**: durante o período mínimo de 3 (três anos), contados a partir da data do recebimento do software ✓ **Vacinas de vírus**: durante o período mínimo de 3 (três anos), contados a partir da data do recebimento do software ✓ **Modalidades de suporte, direto com o**		

			fabricante: deverão ser oferecidas as seguintes modalidades, durante o período mínimo de 3 (três anos), contados a partir da data do recebimento do software**.** ✓ Suporte e atendimento telefônico em português ou inglês. ✓ Suporte e atendimento via chat em português ou inglês. ✓ Suporte e atendimento remoto. ✓ **Licenciamento:** possuir licenciamento para todos os recursos de software, descritos neste Termo de Referência, de no mínimo 3 (três anos). ✓ O fabricante/ fornecedor deverá manter suporte técnico (para resolução de dúvidas e problemas) em português, durante toda a vigência do contrato através dos seguintes meios): • Telefones fixos funcionando em horário comercial (08:30 as 18:00); • Abertura de chamados on line; • Web site na internet; • Email. SPS SESI 1261 (523 unidades) e SPS SENAI 813 (349 unidades)		

VALOR TOTAL ESTIMADO DA PROPOSTA R$ 162.322,80 (Cento e sessenta e dois mil trezentos e vinte e dois reais e oitenta centavos).

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 7.8.): DADOS DO REPRESENTANTE DA EMPRESA (CONFORME ITEM 7.8.): GARANTIA:			

ITEM	QTDE	UN.	DESCRIÇÃO	MARCA	PREÇO UNITÁRIO	PREÇO TOTAL
01	872	UN.	**LICENÇAS DE SOFTWARE ANTIVÍRUS** **Servidor de administração e console administrativa. A Console da solução deve possuir as seguintes características:** • A console de gerenciamento deve ser acessível via Web; • A console de gerenciamento central deverá ser compatível com os ambientes de virtualização: Microsoft Hyper V, VMware vSphere, View, VMware Player, Citrix XenServer, XenDe.sktop, VDI-in-a-Box, Red Hat Enterprise Virtualization, Oracle VM, Kernel-basedVirtual Machine or KVM; • A solução deverá ser integrável com Microsoft Active Directory, Citrix XenServer e VMware vCenter, na descoberta e no gerenciamento das máquinas virtualizadas; • Deve permitir a instalação de mais de 1 Virtual Appliance para cada componente de gerenciamento; • Capacidade de criação de mais de um usuário com			

			privilégios administrativos; • Capacidade de criação de usuários com privilégios apenas para visualização de relatórios; • Capacidade de efetuar logon no console de gerenciamento com as credenciais do Active Directory; • Capacidade de descoberta das máquinas por domínio; • Função especial de "relay" ou retransmissores ilimitados (espalhados pela matriz e escritórios remotos/localidades/filiais) dos pacotes de instalação com as políticas de segurança além das atualizações locais da base de assinaturas de vírus (definições conhecidas de malwares); • Função especial de varredura central com agente leve para a proteção, varredura e remoção de vírus na memória, trilha zero de boot e arquivos dos servidores e estações físicas ou virtuais; • Deve permitir o gerenciamento centralizado através da mesma console de estações, servidores, laptops, mobile e computadores/servidores virtualizados; • Remover automaticamente qualquer software antivírus que houver instalado no computador (estações e servidores) no momento da instalação do Antivírus; • Mecanismo de Comunicação em tempo real, entre servidor e clientes, para entrega de configurações e assinaturas; • Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo e login script; • Capacidade de gerar pacotes customizados (autoexecutáveis) para instalação local nos computadores; • Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;			

			• Capacidade de monitorar diferentes subredes a fim de encontrar máquinas novas para serem adicionadas à proteção; • Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para ser adicionadas à proteção; • Capacidade de instalação e atualização do Software sem intervenção do usuário; • Capacidade de agrupamento de máquina por Grupos ou Estrutura do Active Directory; • Capacidade de definir políticas de configurações diferentes pela estrutura do Active Directory e por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos; • Deve fornecer as seguintes informações dos computadores: ➢ Se o antivírus está instalado; ➢ Se o antivírus está iniciado; ➢ Se o antivírus está atualizado; ➢ Tempo de comunicação desde a última conexão da máquina com o servidor administrativo; ➢ Última atualização de vacinas ➢ Última verificação executada na máquina; ➢ Versão do antivírus instalado na máquina; ➢ Necessidade de reiniciar o computador para aplicar mudanças; ➢ Quantidade de vírus encontrados (contador) na máquina; ➢ Nome do computador; • Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las; • Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação (update Server), sem que seja			

			necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de atualização, a fim de otimizar tráfego da rede; • Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF e XLS e/ou PDF e CSV • Capacidade de enviar E-mails para contas específicas em caso de algum evento; • Capacidade de realizar atualização incremental de vacinas nos computadores clientes; • Capacidade de reiniciar as máquinas remotamente; • Possuir a Tecnologia de analise comportamental de detecção para vírus e ameaças desconhecidas que analisa o comportamento de códigos potencialmente maliciosos dentro de um ambiente virtual seguro de um computador, eliminando os falsos positivos e aumentando as taxas de detecção de malware desconhecidos. • O fabricante da solução ofertada deverá possuir o prêmio/certificado AV Test e não poderá ter recebido notas inferiores a 4,5 em testes feitos nos últimos 12 meses. • O Fabricante/Desenvolvedor da solução deverá obrigatoriamente ser participante do programa MAPP (Microsoft Active Protections Program), garantindo assim o recebimento antecipado de informações sobre vulnerabilidades e segurança sobre a plataforma Microsoft; **Descrição da Proteção para Servidores e Estações de trabalhos** Compatibilidade: ✓ Microsoft Windows 7 ✓ Microsoft Windows 8 ✓ Microsoft Windows 8.1 ✓ Windows 10 ✓ Windows Server 2008			

			✓ Windows Server 2008 R2 ✓ Windows Server 2012 ✓ Windows Server 2012 R2 **Características:** Deve prover as seguintes proteções: • Proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos; • Proteção antispyware deve ser nativa do próprio antivírus, sem necessidade de plugin ou instalação adicional; • AntiPhising (módulo para verificação e classificação de sites e downloads contra vírus); • Verificação de vírus nas mensagens de correio eletrônico, suportando clientes Outlook; • Permitir o escaneamento das ameaças de maneira manual, agendado ou em tempo real, detectando ameaças no nível do Kernel do Sistema Operacional com capacidade de detecção de rootkits; • Permitir o isolamento de arquivos, para área de quarentena, para serem enviados e vistoriados pelo centro de pesquisa do fabricante; • Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo, reparar, apagar, mover para área de isolamento e ignorar; • Deve possui Firewall que suporte os protocolos TCP, UDP e ICMP no mínimo; • Autoproteção (contra-ataques aos serviços/processos do antivírus); • Controle de execução de aplicativos; • Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota; • As vacinas devem ser atualizadas pelo fabricante e disponibilizadas via servidor central de gerenciamento, podendo ser configurada a base de			

			atualização como primeira atualização, em caso de falha do servidor de atualização principal, as estações devem buscar a atualizações no site do fabricante, sendo possível configurar a hora de atualização nas estações e proxy; • Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução; • Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, removendo a solução no momento da instalação do antivírus; • Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão com o Nome do arquivo para que qualquer objeto detectado escolhido seja ignorado; • Capacidade de verificar arquivos zipados (incluindo .zip, rar); • Capacidade de verificar objetos usando heurística; • O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: ➢ Perguntar o que fazer, ou; ➢ Bloquear acesso ao objeto; ➢ Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador); ➢ Em caso positivo de desinfecção, restaurar o objeto para uso; ➢ Em caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador); ➢ Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;			

			• Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3 e SMTP; • Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings; • Capacidade de verificar links inseridos em e-mails contra phishings; • Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox, Safari e Chrome; • Possibilidade de verificar e-mails enviados e recebidos; • Capacidade de filtrar anexos de e-mail, apagando-os de acordo com a configuração feita pelo administrador; • Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas; • Na verificação de tráfego web, caso encontrado código malicioso o programa deve: ➢ Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio; ➢ Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou; ➢ Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação; • Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web; • Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas; • Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade			

			maliciosa; • Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas; • Deve possuir módulo Firewall para proteção contra exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas; • O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: ➢ Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; ➢ Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo ou nome de aplicativo terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados; ➢ Opção de Criar Perfis de Rede ou Zonas; ➢ Controle de Conexão; ➢ Deve possuir o Modo Invisível onde em caso de tentativa de Port Scan a maquinas parem de responder e fiquem invisível a tentativa de escaneamento; • Capacidade de limitar a execução de aplicativos por nome do arquivo ou hash. (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc.); • Capacidade de, caso o computador cliente saia da rede corporativa, possa atualizar as vacinas via site do fabricante e manter as regras originadas da Console de gerenciamento. • Prover módulo onde o usuário consiga alterar qualquer configuração do antivírus de forma local; • Capacidade de ter escaneamento hibrido, tanto com o servidor que está na internet, quanto via servidor local. Esse servidor local deve ser virtualizado e armazenar grande parte do motor do antivírus para melhorar a performance da estação			

			com poucos recursos disponíveis. • Deve possuir módulo para bloqueio de dispositivos, com no mínimo os seguintes itens: ➢ Bluetooth ➢ CDROM ➢ Drive de disquete ➢ IEEE 1284.4 ➢ IEEE 1394 ➢ Modem ➢ Drives de fita ➢ Portas COM/LPT ➢ Discos SCSI em Raid ➢ Impressoras ➢ Adaptadores de rede ➢ Adaptadores de rede Wireless ➢ Armazenamento interno ➢ Armazenamento externo **Descrição das Estações de Trabalho Linux** Compatibilidade: • Plataforma 32/64bits: • Red Hat Enterprise Linux / CentOS 5.6 ou superior • Ubuntu 11.04 LTS ou superior • OpenSUSE 11 ou superior • Fedora 16 ou superior • Debian 6.0 ou superior **Características:** Deve prover as seguintes proteções: • Antivírus de arquivos (AntiSpyware, AntiTrojan, AntiMalware); • Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: ➢ Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); ➢ Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;			

			➢ Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares; ➢ Capacidade de verificar arquivos compactados em até 20 níveis; ➢ Capacidade de verificar arquivos compactados em até 80 tipos de formatos; ➢ Capacidade de verificar objetos usando heurística; • Deve possuir integração com o módulo de administração Central ou através de ferramenta nativa; **Descrição da Proteção para Servidores de E-mails Exchange** Características • Compatibilidade com Servidores Exchange 2007/2010/2013 • Deve possuir as seguintes características: • Deve Possuir os Filtros de AntiSpam, Antiphishing, Antispyware e Filtragem de Conteúdo; • Capacidade de verificar todos os e-mails enviados e recebidos contra vírus, Trojan, spyware e qualquer tipo de código malicioso e potencialmente hostil em anexos e no corpo do e-mail; • Capacidade de varrer o sistema de arquivos do servidor sob demanda; • Capacidade de verificar somente objetos novos ou alterados; • Capacidade de filtrar anexos por nome e tipo de arquivo; • Capacidade de filtrar anexos por nome e tipo de arquivo e bloquear o recebimento ou envio do mesmo de acordo com as regras do Administrador;			

			• Capacidade de agrupar usuários e criar regras por grupos; • Capacidade de armazenar cópias de arquivo infectado antes da tentativa de desinfecção; • Capacidade de colocar em quarentena arquivos suspeitos ou danificados; • Possuir Filtro Bayesiano de classificação de Mensagens • Capacidade de enviar notificações de objetos suspeitos e infectados para o administrador, remetente e destinatário da mensagem; • Deve possuir atualização de vacinas automáticas e sob demanda. O fabricante deve submeter novas atualizações com frequência horária, independentemente do nível de ameaça sendo possível configurar o intervalo de agendamento de horários de atualização das Vacinas e Produto; **Descrição da Proteção para Mobiles** Compatibilidade: • Smartphones e Tablets Android 2.2 ou Superior; • Smartphones e Tablets iOS 5 ou Superior **Características:** Deve prover as seguintes proteções: • Antivírus de arquivos residente (AntiSpyware, AntiTrojan, AntiMalware, antiSpam) que verifique qualquer arquivo criado, acessado ou modificado. As vacinas devem ser atualizadas pelo fabricante; • Capacidade de bloquear a tela do dispositivo com senha; • Capacidade de apagar os dados do dispositivo em caso de perda ou roubo do aparelho; • Capacidade de descobrir a localização do aparelho em caso de perda ou roubo; • Capacidade de escaneamento em tempo real e criptografia para dispositivos Android; • Capacidade de gerenciamento integrado com Microsoft Active Directory;			

			Descrição da Proteção para Servidores e Estações de trabalho virtualizados • Plataforma de virtualização suportada: • VMware vSphere 6, VMware vSphere 5.1, 5.0, 4.1 com VMware vCenter Server 6.0, 5.1, 5.0, 4.1 • VMware View 5.1, 5.0 • Microsoft Hyper-V Server 2008 R2 • Microsoft Hyper-V Server 2012 • Microsoft Hyper-V Server 2012 R2 **Sistemas operacionais suportados para proteção em virtualização:** • Fedora 16, 15 • SUSE Linux Enterprise Server 11 • Ubuntu 12.04 • Red Hat Enterprise Linux / CentOS 6.2, 6.1, 5.7, 5.6 • Windows Vista • Windows 7 • Windows 8 • Windows Server 2003 • Windows Server 2003 R2 • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 **Características:** Deve prover as seguintes proteções: • Capacidade de proteger máquinas virtuais através da integração com VMware vShield Endpoint sem necessidade de instalação de agentes; • Capacidade de fazer o escaneamento nas máquinas virtuais através da integração com VMware Vshield Endpoint instalados mesmo com a máquina virtual off-line; • Capacidade de proteger ambiente virtualizado em qualquer plataforma de virtualização instalada;			

			• Capacidade de proteger arquivos de sistema, processos e memória em Windows e Linux; • Capacidade de realizar escaneamento das máquinas que estão desligadas (escaneamento off-line); • Antivírus de Arquivos residente (antispyware, antitrojan, antimalware, etc.) que verifique qualquer arquivo criado, acessado ou modificado; • As vacinas devem ser atualizadas pelo fabricante; • Capacidade de verificar arquivos compactados com a opção de colocar quantos níveis de compactação deve ser o escaneamento; • Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.); • Capacidade de verificar objetos usando heurística; • Capacidade de configurar diferentes ações para diferentes tipos de ameaças; • Caso o Servidor seja File Server, instalar além do agente o Módulo de File Server onde deverá mostrar as seguintes informações por dia, semana ou mês: **b)** Itens analisados, Itens infectados, Itens suspeitos, Itens limpos, Itens não analisados, vírus individuais, Riskware individual, spyware, adware, aplicações, discadores, Itens resolvidos, desinfectado, apagado, movido para quarentena, acesso bloqueado, ignorado; Capacidade de atualizar o módulo de proteção sem reiniciar o servidor. **Suporte, Manutenção e Licenciamento** ✓ **Garantia:** pelo prazo de 3 (três) anos, contados a partir da data da entrega do software, isentando o SESI/SENAI de qualquer ônus decorrente de falhas do software durante o período contratado, salvo condições de uso e manipulação indevidas por			

			parte do SESI/SENAI. ✓ **Atualizações de software**: durante o período mínimo de 3 (três anos), contados a partir da data do recebimento do software ✓ **Vacinas de vírus**: durante o período mínimo de 3 (três anos), contados a partir da data do recebimento do software ✓ **Modalidades de suporte, direto com o fabricante**: deverão ser oferecidas as seguintes modalidades, durante o período mínimo de 3 (três anos), contados a partir da data do recebimento do software**.** ✓ Suporte e atendimento telefônico em português ou inglês. ✓ Suporte e atendimento via chat em português ou inglês. ✓ Suporte e atendimento remoto. ✓ **Licenciamento:** possuir licenciamento para todos os recursos de software, descritos neste Termo de Referência, de no mínimo 3 (três anos). ✓ O fabricante/ fornecedor deverá manter suporte técnico (para resolução de dúvidas e problemas) em português, durante toda a vigência do contrato através dos seguintes meios): • Telefones fixos funcionando em horário comercial (08:30 as 18:00); • Abertura de chamados on line; • Web site na internet; • Email. SPS SESI 1261 (523 unidades) e SPS SENAI 813 (349 unidades)			

VALOR TOTAL DA PROPOSTA R$ _____ (_____)

CONDIÇÕES GERAIS

DA FORMA DE ENTREGA E RECEBIMENTO

O recebimento das licenças dar-se-ão da seguinte forma:

- ✓ No momento da entrega das licenças será emitido o Termo de Recebimento Provisório – TRP, pela Gerência de Tecnologia da Informação, para posterior emissão do Termo de Recebimento Definitivo – TRD, que se dará em até 15 (quinze) dias corridos, contados da emissão do TRP.
- ✓ A Gerência de Tecnologia da Informação – GTI do Sistema Fibra somente emitirá o Termo de Recebimento Definitivo – TRD das licenças antivírus quando comprovado o atendimento das especificações técnicas e demais condições solicitadas.
- ✓ As licenças antivírus entregues em desacordo com as especificações técnicas e demais condições estabelecidas neste Edital serão recusados e deverão ser substituídos em até 30 (trinta) dias por outros que atendam às especificações técnicas, sem acréscimo de valores para a Contratante.

CRONOGRAMA DE DESEMBOLSO FINANCEIRO										
Objeto: Aquisição de software antivírus 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 licenças de software antivírus para proteção de rede corporativa do Sistema Fibra.	872	UND			R$ 162.322,80						
Valor Total (R$)			**R$ 0,00**	**R$ 0,00**	**R$ 162.322,80**	**R$ 0,00**	**R$ 0,00**	**R$ 0,00**	**R$ 0,00**	**R$ 0,00**	**R$ 0,00**

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

Declaro(amos) sob as penas da lei, que a (nome da pessoa jurídica) assume o compromisso da garantia mínima de 3 (três) anos para os objetos ofertados no **Pregão Eletrônico nº 08/2016,** do SERVIÇO SOCIAL DA INDÚSTRIA – SESI/DR-DF e SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL SENAI/DR-DF – Departamentos Regionais do Distrito Federal, 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)