MINISTÉRIO DA EDUCAÇÃO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

EDITAL

PREGÃO ELETRÔNICO Nº. 19/2013

(Processo Administrativo n°. 23060.003025/2012-06)

HABILITAÇÃO COMPLETA (ART. 8º, II, III, IV, V E VI DA IN SLTI/MPOG Nº 2, DE 11.10.10)

Data da abertura da sessão para análise das propostas:

06/08/2013 às 09h:00min.

Local: http://comprasnet.gov.br

Endereço para correspondências: Av. Jorge Amado, 1551 – Loteamento Garcia, Bairro Jardins, CEP: 49.025-330. Aracaju-SE

Torna-se público, para conhecimento dos interessados, que o **Instituto Federal de Educação, Ciência e Tecnologia de Sergipe** – IFS, sob CNPJ 10.728.444/0001-00, por meio do Departamento de Li

citações e Contratos mediante o pregoeiro **Agnaldo dos Santos**, designado pela Portaria nº. 0627, de 07 de março de 2013, sediado na Av. Jorge Amado, 1551, Loteamento Garcia, Bairro Jardins, CEP: 49025-330 realizará licitação, na modalidade **PREGÃO,** na forma **ELETRÔNICA,** do **TIPO MENOR PREÇO,** por grupo, nos termos da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 5.450, de 31 de maio de 2005, das Instruções Normativas SLTI/MPOG nº 1, nº 2 e nº 4, de 19 de janeiro de 2010, de 11 de outubro de 2010 e 12 de novembro de 2010, respectivamente, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 6.204, de 05 de setembro de 2007, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993, com suas alterações posteriores, demais ditames legais aplicáveis à matéria e as exigências estabelecidas neste Edital.

1. ENVIO DAS PROPOSTAS

1.1. O encaminhamento das propostas terá início com a divulgação do aviso de Edital no sítio www.comprasnet.gov.br, até às 09:00 horas do dia 06/08/2013, hora e data para a abertura da sessão, exclusivamente por meio do sistema eletrônico;

1.2. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF;

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

ANEXO I – Termo de Referência;

ANEXO II – Modelos de Declarações;

ANEXO III – Modelo de Declaração de Sustentabilidade Ambiental;

ANEXO IV – Modelo de Proposta de Preços;

ANEXO V – Minuta de Contrato

2. DO OBJETO

2.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de serviços de aquisição, renovação e treinamento no uso de licenças de software de antivírus com garantia e prestação de serviço de suporte**,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

2.2. A licitação será processada com 1 (um) grupo, formado por 2 (dois) itens, conforme tabela constante do item 1.1 do Termo de Referência, devendo o licitante ofertar proposta para todos os itens que o compõe.

3. DOS RECURSOS ORÇAMENTÁRIOS

3.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento da União para o exercício de 2013, na classificação abaixo:

Gestão/Unidade: 158134

Fonte: 0112000000

Programa de Trabalho: 12363203120RL0028

PI: A2992P0100P

Elemento de Despesa: 44.90.39-93

Elemento de Despesa: 33.90.39.48

4. DO CREDENCIAMENTO

4.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

4.2. O cadastro no SICAF poderá ser iniciado no Portal de Compras do Governo Federal – Comprasnet, no sítio www.comprasnet.gov.br, com a solicitação de login e senha pelo interessado.

4.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

4.4. O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema, ou ao órgão ou entidade responsável por esta licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

4.5. A perda da senha ou a quebra de sigilo deverá ser comunicada imediatamente ao provedor do sistema para imediato bloqueio de acesso.

5. DA PARTICIPAÇÃO NO PREGÃO.

5.1. Poderão participar deste Pregão entidades empresariais cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no §3º do artigo 8º da IN SLTI/MPOG nº 2, de 2010.

5.2. Não poderão participar desta licitação:

5.2.1. entidades empresariais proibidas de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

5.2.2. entidades empresariais declaradas suspensas de participar de licitações e impedidas de contratar com o órgão ou a entidade responsável por esta licitação, conforme art. 87, inciso III, da Lei nº 8.666, de 1993;

5.2.3. entidades empresariais estrangeiras que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

5.2.4. quaisquer interessados que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

5.2.5. entidades empresariais que estejam sob falência, em recuperação judicial ou extrajudicial, concurso de credores, concordata ou insolvência, em processo de dissolução ou liquidação;

5.2.6. entidades empresariais que estejam reunidas em consórcio sejam controladoras, coligadas ou subsidiárias entre si.

5.3. Como condição para participação no Pregão, o licitante assinalará "sim" ou "não" em campo próprio do sistema eletrônico, relativo às seguintes declarações:

5.3.1. que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;

5.3.1.1. a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte.

5.3.2. que está ciente e concorda com as condições contidas no Edital e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no Edital;

5.3.3. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

5.3.4. que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

5.3.5. que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MPOG nº 2, de 16 de setembro de 2009.

6. DO ENVIO DA PROPOSTA

6.1. O licitante deverá encaminhar a proposta por meio do sistema eletrônico até a data e horário marcados para abertura da sessão, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas.

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

6.3. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

6.4. Até a abertura da sessão, os licitantes poderão retirar ou substituir as propostas apresentadas.

6.5. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, em conformidade com o Formulário de Proposta anexo a este edital, dos seguintes campos:

6.5.1. valor total do item;

6.5.2. descrição detalhada do objeto.

6.5.2.1. Quando do registro das propostas no Sistema Eletrônico, as licitantes deverão observar a orientação estabelecida pelo Ministério do Planejamento, Orçamento e Gestão, no sentido de incluir o detalhamento do objeto ofertado no campo **"Descrição Detalhada do Objeto"**.

6.5.2.1.1. Serão desclassificadas as propostas que não apresentarem a descrição de forma clara e objetiva, tal qual a contida no Termo de Referência, **vedadas descrições do tipo "Conforme Edital".**

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

6.7. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços.

6.8. O prazo de validade da proposta não será inferior a 60 (sessenta) dias**,** a contar da data de sua apresentação.

7. DAS PROPOSTAS E FORMULAÇÃO DE LANCES

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

7.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência ou ainda apresentem expressões como "conforme o edital" e similares.

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

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

7.3. Não será admitida a desistência da proposta/lance, após o **INÍCIO ou ENCERRAMENTO da fase de lances.**

7.3.1. EXCEPCIONALMENTE, após o ENCERRAMENTO da fase de lances poderá ser acatado o pedido de desistência da proposta, em razão de motivo justo devidamente comprovado pela LICITANTE, decorrente de fato superveniente, e aceito pelo Pregoeiro.

7.3.2. Não restando comprovado o atendimento aos requisitos fixados no subitem 7.3.1 acima, a LICITANTE DESISTENTE ficará sujeita à aplicação das sanções previstas neste Edital.

7.4. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

7.5. O sistema disponibilizará campo próprio para troca de mensagem entre o Pregoeiro e os licitantes.

7.6. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.6.1. O lance deverá ser ofertado pelo valor total do item.

7.6.1.1. A cada lance ofertado (**por item**), o sistema eletrônico atualizará automaticamente o valor global do GRUPO, sagrando-se vencedora a licitante que ofertar o **Menor Valor Global do GRUPO.**

7.7. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas neste Edital.

7.8. O licitante somente poderá oferecer lance inferior ao último por ele ofertado e registrado pelo sistema.

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

7.10. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

7.11. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.12. Se a desconexão perdurar por tempo superior a 10 (dez) minutos, a sessão será suspensa e terá reinício somente após comunicação expressa do Pregoeiro aos participantes.

7.13. A etapa de lances da sessão pública será encerrada por decisão do Pregoeiro. O sistema eletrônico encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado pelo sistema, findo o qual será automaticamente encerrada a recepção de lances.

7.14. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta e, na hipótese de desistência de apresentar outros lances, valerá o último lance por ele ofertado, para efeito de ordenação das propostas.

7.15. Encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 6.204, de 2007.

7.16. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da proposta ou lance de menor preço serão consideradas empatadas com a primeira colocada.

7.17. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

7.18. Caso a microempresa ou empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.19. Caso não se oferte lances e sejam identificadas propostas de preços idênticos de Microempresa ou Empresa de Pequeno Porte empatadas na faixa de até 5% (cinco por cento) sobre o valor cotado pela primeira colocada, e permanecendo o empate até o encerramento do grupo, o sistema fará sorteio eletrônico entre tais fornecedores, definindo e convocando automaticamente o vencedor para o encaminhamento da oferta final de desempate.

7.20. Havendo êxito no procedimento de desempate, o sistema disponibilizará a nova classificação de fornecedores para fins de aceitação do valor ofertado. Não sendo aplicável o procedimento, ou não havendo êxito na aplicação deste, prevalecerá a classificação inicial.

7.21. Mantido o empate entre propostas, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos serviços:

7.21.1. prestados por empresas brasileiras;

7.21.2. prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País.

7.22. Persistindo o empate, o critério de desempate será o sorteio, em ato público para o qual os licitantes serão convocados, vedado qualquer outro processo.

8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

8.1. Encerrada a etapa de lances e depois da verificação de possível empate, o Pregoeiro examinará a proposta classificada em primeiro lugar para fim de aceitação.

8.2. Será desclassificada a proposta ou o lance vencedor com valor superior ao preço máximo fixado, ou que apresentar preço manifestamente inexequível, assim considerado aquele que não venha a ter demonstrada sua viabilidade através de documentação que comprove que os custos são coerentes com os de mercado.

8.3. Para efeito de aceitabilidade da menor proposta ou menor lance, considera-se manifestamente inexequível, aquele que, comprovadamente, for insuficiente para a cobertura dos custos decorrentes da contratação.

8.4. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993, a exemplo das enumeradas no § 3º, do art. 29, da IN SLTI/MPOG nº 2, de 2008.

8.5. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, não sendo possível a sua imediata desclassificação por inexequibilidade, será obrigatória a realização de diligências para o exame da proposta.

8.6. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

8.7. O Pregoeiro poderá convocar o licitante para enviar documento digital, por meio de funcionalidade disponível no sistema, estabelecendo no "chat" prazo razoável para tanto, sob pena de não aceitação da proposta.

8.7.1. O prazo estabelecido pelo Pregoeiro poderá ser prorrogado por solicitação escrita e justificada do licitante, formulada antes de findo o prazo estabelecido, e formalmente aceita pelo Pregoeiro.

8.8. Se a proposta ou lance de menor valor não for aceitável, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

8.9. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "*chat*" a nova data e horário para a continuidade da mesma.

8.10. O Pregoeiro poderá encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.

8.10.1. Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

8.10.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

8.11. Sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

9. DA HABILITAÇÃO

9.1. O Pregoeiro consultará o Sistema de Cadastro Unificado de Fornecedores – SICAF, em relação à habilitação jurídica, à regularidade fiscal e à qualificação econômica financeira, conforme disposto nos arts. 4º, *caput*, 8º, § 3º, 13 a 18 e 43 da Instrução Normativa SLTI/MPOG nº 2, de 2010.

9.1.1. Também poderão ser consultados os sítios oficiais emissores de certidões, especialmente quando o licitante esteja com alguma documentação vencida junto ao SICAF.

9.1.2. Caso o Pregoeiro não logre êxito em obter a certidão correspondente através do sítio oficial, o licitante será convocado a encaminhar, no prazo de 3 (três) horas, documento válido que comprove o atendimento das exigências deste Edital, sob pena de inabilitação, ressalvado o disposto quanto à comprovação da regularidade

fiscal das microempresas empresas de pequeno porte, conforme estatui o art. 43, § 1º da LC nº 123, de 2006.

9.2. Os licitantes que não estiverem cadastrados no Sistema de Cadastro Unificado de Fornecedores – SICAF além do nível de credenciamento exigido pela Instrução Normativa SLTI/MPOG nº 2, de 2010, deverão apresentar a seguinte documentação relativa à Habilitação Jurídica e à Regularidade Fiscal, nas condições seguintes:

9.3. Habilitação jurídica:

9.3.1. no caso de empresário individual, inscrição no Registro Público de Empresas Mercantis;

9.3.2. em se tratando de sociedades comerciais, contrato social ou estatuto em vigor, devidamente registrado, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;

9.3.3. inscrição no Registro Público de Empresas Mercantis onde opera com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

9.3.4. inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas, no caso de sociedades simples, acompanhada de prova de diretoria em exercício;

9.3.5. decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

9.4. Regularidade fiscal e trabalhista:

9.4.1. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

9.4.2. prova de regularidade com a Fazenda Nacional (certidão conjunta, emitida pela Secretaria da Receita Federal do Brasil e Procuradoria-Geral da Fazenda Nacional, quanto aos demais tributos federais e a Divida Ativa da União, por elas administrados, conforme art. 1º, inciso I, do Decreto nº 6.106/07);

9.4.3. prova de regularidade com a Seguridade Social (INSS);

9.4.4. prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.4.5. prova de inscrição no cadastro de contribuintes municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.4.6. prova de regularidade com a Fazenda Estadual e Municipal do domicílio ou sede do licitante;

9.4.6.1. caso o fornecedor seja considerado isento dos tributos estaduais e/ou municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal do domicílio ou sede do fornecedor, ou outra equivalente, na forma da lei.

9.4.7. prova de inexistência de débitos trabalhistas, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas (CNDT), expedida conforme art. 642-A da Consolidação das Leis do Trabalho (artigo introduzido por meio da Lei nº 12.440, de 7/07/2011), nos termos do art. 27, inciso IV da Lei nº 8.666/93 e caso não a tenha esta poderá ser substituída por Certidão Positiva com Efeitos de Negativa;

9.4.8. caso o licitante detentor do menor preço, por grupo, seja microempresa ou empresa de pequeno porte, deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

9.5. Os licitantes que não estiverem cadastrados no Sistema de Cadastro Unificado de Fornecedores – SICAF no nível da Qualificação Econômico-Financeira, conforme Instrução Normativa SLTI/MPOG nº 2, de 2010, deverão apresentar a seguinte documentação:

9.5.1. certidão negativa de falência ou recuperação judicial expedida pelo distribuidor da sede da pessoa jurídica;

9.5.2. balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

9.5.2.1. no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

9.5.3. comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), resultantes da aplicação das fórmulas:

$$LG = \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}};$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}};$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}; \text{ e}$$

9.5.4. As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar que:

9.5.4.1. possuem capital social de 10 (dez por cento) do valor estimado da contratação;

9.5.5. Qualificação Técnica:

9.5.5.1. Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o grupo pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado;

9.5.5.2. Os atestados referir-se-ão a contratos já concluídos ou já decorrido no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior, apenas aceito mediante a apresentação do contrato;

9.5.5.3. Todos os técnicos de suporte da contratada devem ser capacitados e certificados, pelo fabricante dos produtos a prestar atendimento de suporte técnico;

9.5.5.4. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados.

9.6. Os documentos exigidos para habilitação relacionados nos subitens acima, deverão ser apresentados pelos licitantes, via fac-símile (fax) número (79)-3711-3183, ou via e-mail **copem.delc@hotmail.com.br**, **copem@ifs.edu.br**, no prazo de 01 (uma) hora, após solicitação do Pregoeiro no sistema eletrônico. Posteriormente, serão remetidos em original, por qualquer processo de cópia reprográfica, autenticada por tabelião de notas, ou por servidor da Administração, desde que conferido(s) com o original, ou publicação em órgão da imprensa oficial, para análise, num prazo máximo de 05 (cinco) dias corridos, depois de encerrado o prazo para o encaminhamento via fax símile (fax) ou e-mail;

9.7. Se a menor proposta ofertada for de microempresa ou empresa de pequeno porte e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal, a mesma será convocada para, no prazo de 2 (dois) dias úteis, após solicitação do Pregoeiro no sistema eletrônico, comprovar a regularização. O prazo poderá ser prorrogado por igual período.

9.7.1. A não regularização fiscal no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa ou empresa de pequeno porte com alguma restrição na documentação fiscal, será concedido o mesmo prazo para regularização.

9.8. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

9.9. Será inabilitado o licitante que não comprovar sua habilitação, deixar de apresentar quaisquer dos documentos exigidos para a habilitação, ou apresentá-los em desacordo com o estabelecido neste Edital.

9.10. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.11. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

10. DOS RECURSOS

10.1. O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal de microempresa ou empresa de pequeno, se for o caso, concederá o prazo de no mínimo 20 (vinte) minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual (is) decisão (ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

10.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

10.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

10.3. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito e a consequente adjudicação do objeto pelo Pregoeiro ao licitante vencedor.

10.3.1. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de 3 (três) dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

10.4. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

10.5. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

11. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

11.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

11.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

12. DA GARANTIA DE EXECUÇÃO

12.1. O adjudicatário, no prazo de 10 (dez) dias úteis, após a assinatura do Termo de Contrato, prestará garantia no valor correspondente a 5% (cinco por cento) do valor do Contrato, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 56 da Lei nº 8.666, de 1993, desde que cumpridas às obrigações contratuais.

12.2. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de mais de 3 (três) meses após o término da vigência contratual.

12.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

12.3.1. prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

12.3.2. prejuízo causados à Contratante ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

12.3.3. as multas moratórias e punitivas aplicadas pela Contratante à Contratada.

12.3.4. Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela CONTRATADA.

12.4. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, até o máximo de 2% (dois por cento).

12.5. A garantia em dinheiro deverá ser efetuada na Caixa Econômica Federal, em conta específica com correção monetária, em favor do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe.

12.6. A Contratante não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses:

12.6.1. caso fortuito ou força maior;

12.6.2. alteração, sem prévia anuência da seguradora, das obrigações contratuais;

12.6.3. descumprimento das obrigações pelo contratado decorrentes de atos ou fatos praticados pela Contratante;

12.6.4. atos ilícitos dolosos praticados por servidores da Contratante.

12.7. Cabe à própria Contratante apurar a isenção da responsabilidade prevista nas alíneas acima, não sendo a entidade garantidora parte no processo instaurado pela Contratante.

12.8. Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas neste item.

12.9. Será considerada extinta a garantia:

12.9.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

12.9.2. no prazo de 90 (noventa) após o término da vigência, caso a Contratante não comunique a ocorrência de sinistros.

13. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

13.1. Após a homologação da licitação, será firmado Termo de Contrato ou aceito instrumento equivalente (Nota de Empenho/Carta Contrato/Autorização), cujo prazo de

vigência é de 36 (trinta e seis) meses, prorrogável na forma do art. 57, § 1°, da Lei n° 8.666/93.

13.2. O adjudicatário terá o prazo de 5 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar o instrumento equivalente, conforme o caso, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

13.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite do adjudicatário, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado ou aceito no prazo de 5 (cinco) dias úteis, a contar da data de seu recebimento.

13.3. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

13.4. Antes da assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração realizará consulta "*on line*" ao SICAF, ao Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa (www.cnj.jus.br), ao CEIS - Cadastro de Empresas Inidôneas ou Suspensas (www.portaltransparencia.gov.br), ao TST / CNDT – Certidão Negativa de Débitos Trabalhistas – (www.tst.jus.br), cujos resultados serão anexados aos autos do processo.

13.5. Se o adjudicatário, no ato da assinatura do Termo de Contrato ou aceite do instrumento equivalente, não comprovar que mantém as mesmas condições de habilitação, ou quando, injustificadamente, recusar-se à assinatura ou aceite, poderá ser convocado outro licitante, desde que respeitada à ordem de classificação, para, após a verificação da aceitabilidade da proposta, negociação e comprovados os requisitos de habilitação, celebrar a contratação, sem prejuízo das sanções previstas neste Edital e das demais cominações legais.

14. DO REAJUSTE

14.1. Os preços são fixos e irreajustáveis.

15. DA ENTREGA E SEU RECEBIMENTO

15.1. A entrega dos itens deverá ser realizada pelo licitante vencedor, no endereço: Reitoria, Av. Jorge Amado, 1551 – Loteamento Garcia – Bairro Jardins – CEP: 49025-330,

Aracaju-SE, Divisão de Patrimônio, no prazo máximo de 20 (vinte) dias corridos, após a assinatura do contrato ou instrumento equivalente.

15.2. O recebimento das licenças será provisório, para posterior teste de conformidade e verificação das especificações técnicas constantes do Termo de Referência – ANEXO I.

15.3. O IFS efetuará os testes de conformidade e verificação das licenças, em até 15 (quinze) dias após o recebimento provisório, para que seja configurado o recebimento definitivo e para que seja lavrado o termo de aceite momento no qual será recebido definitivamente o serviço:

15.3.1. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

15.4. O (s) material (ais) será (ao) recusado(s) se entregue(s) com as especificações técnicas diferentes das contidas neste Termo de Referência e na proposta.

15.5. A licitante vencedora terá o prazo de 72 (setenta e duas) horas corridas para providenciar a substituição da(s) licença(s) recusada(s) sem ônus para a Administração e sem prejuízo da aplicação de penalidade. Neste caso, o IFS terá novo prazo para testar a(s) licença(s).

15.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato.

16. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

16.1. Obrigações da Contratante:

16.1.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

16.1.2. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

16.1.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

16.1.4. Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas no Edital e seus anexos;

16.1.5. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura fornecida pela contratada.

16.2. Obrigações da Contratada:

16.2.1. Proceder à entrega dos itens adjudicados, de conformidade com o quantitativo e as especificações constantes do item 1.1 do presente Termo de Referência e da sua proposta comercial.

16.2.2. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer as atualizações do software pelo período de 36 (trinta e seis) meses, na qualidade e quantidade especificadas neste Termo de Referência e em sua proposta.

16.2.3. Providenciar a troca, às suas expensas, dos materiais entregues com defeitos de fabricação e que não correspondam às especificações solicitadas, no prazo máximo de 03 (três) dias.

16.2.4. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrente de sua culpa ou dolo durante o período de entrega dos materiais, não implicando co-responsabilidade do Poder Público ou de seus agentes ou prepostos.

16.2.5. Responder por todo o ônus decorrente do transporte de embalagem, seguros, taxas, fretes e demais encargos que venham incidir na entrega dos materiais.

16.2.6. Lançar na nota fiscal as especificações dos materiais, de modo idêntico àquelas constantes do objeto do Edital de Pregão.

16.2.7. Não transferir a terceiros, total ou parcial, o fornecimento dos materiais sem a prévia e expressa anuência da Contratante.

16.2.8. A CONTRATADA deverá prover atualizações de todas as soluções fornecidas, inclusive upgrades de versões quando as antigas são descontinuadas durante o período de 36 (trinta e seis) meses, sem ônus adicional à CONTRATANTE, inclusive quanto à manutenção e suporte.

16.2.9. A CONTRATADA deverá prestar os serviços em até 20 (vinte) dias após a assinatura deste contrato compreendendo a entrega das licenças e o respectivo treinamento dos servidores.

17. DO PAGAMENTO

17.1. O pagamento será efetuado pela Contratante no prazo de 15 (quinze) dias, contados da apresentação da Nota Fiscal/Fatura contendo o detalhamento dos serviços executados e os materiais empregados.

17.1.1. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

17.2. A apresentação da Nota Fiscal/Fatura deverá ocorrer no prazo de 5 (cinco) dias, contado da data final do período de adimplemento da parcela da contratação a que aquela se referir.

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

17.3. O pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação aos serviços efetivamente prestados e aos materiais empregados.

17.4. O pagamento será efetuado através de ordem bancária, para crédito em banco, agência e conta-corrente indicados pela Contratada.

17.5. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária.

17.6. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

17.6.1. A Contratada regularmente optante pelo Simples Nacional não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

17.7. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \qquad I = \frac{(6/100)}{365} \qquad I = 0{,}00016438$$

TX = Percentual da taxa anual = 6%.

18. DAS SANÇÕES ADMINISTRATIVAS.

18.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

18.1.1. não assinar a ata de registro de preços quando convocado dentro do prazo de validade da proposta ou não assinar o termo de Contrato decorrente da ata de registro de preços;

18.1.2. apresentar documentação falsa;

18.1.3. deixar de entregar os documentos exigidos no certame;

18.1.4. ensejar o retardamento da execução do objeto;

18.1.5. não mantiver a proposta;

18.1.6. cometer fraude fiscal;

18.1.7. comportar-se de modo inidôneo.

18.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

18.3. A licitante/Adjudicatária que cometer quaisquer das infrações discriminadas no subitem anterior ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes **sanções**:

18.3.1. multa de 10% (dez por cento) sobre o valor estimado do(s) item(ns) prejudicado(s) pela conduta do licitante;

18.3.2. impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até 5 (cinco) anos;

18.4. A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.

18.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

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

18.7. As penalidades serão obrigatoriamente registradas no SICAF.

18.8. As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

19. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

19.1. Até 02 (dois) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

19.2. A impugnação poderá ser realizada por forma eletrônica, pelo e-mail copem.delc@hotmail.com.br, copem@ifs.edu.br, pelo fax (79) 3711-3183, ou por petição dirigida ou protocolizada no endereço: Av. Jorge Amado, 1551 – Loteamento Garcia – Bairro Jardins, CEP: 49025-330, no Departamento de Licitações e Contratos.

19.3. Caberá ao Pregoeiro decidir sobre a impugnação no prazo de até 24 (vinte e quatro) horas.

19.4. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

19.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.

19.6. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

19.7. As respostas às impugnações e os esclarecimentos prestados pelo Pregoeiro serão entranhados nos autos do processo licitatório e estarão disponíveis para consulta por qualquer interessado.

20. DAS DISPOSIÇÕES GERAIS

20.1. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

20.2. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

20.3. A homologação do resultado desta licitação não implicará direito à contratação.

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

20.5. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

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

20.7. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

20.8. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerão as deste Edital.

20.9. O Edital está disponibilizado, na íntegra, no endereço eletrônico www.ifs.edu.br, e também poderão ser lidos e/ou obtidos no endereço: Av. Jorge Amado, 1551, Loteamento Garcia, Bairro Jardins, CEP: 49.025-330, no Departamento de Licitações e Contratos, nos dias úteis, no horário das 08h:00min às 12h:00min e das 14h:00min às 17h:00min, no mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

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

20.10.1. ANEXO I – Termo de Referência;

20.10.2. ANEXO II – Modelos de Declarações;

20.10.3. ANEXO III – Modelo de Declaração de Sustentabilidade Ambiental;

20.10.4. ANEXO IV – Modelo de Proposta de Preços;

20.10.5. ANEXO V – Contrato;

Aracaju, 16 de julho de 2013.

Agnaldo dos Santos

Pregoeiro Oficial - IFS

ANEXO I – TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO Nº 19/2013

(Processo Administrativo n°. 23060.003025/2012-06)

1. DO OBJETO

1.1. A presente contratação tem por objeto a aquisição, renovação e treinamento no uso de licença de software antivírus com garantia e prestação de serviço de suporte, conforme condições, quantidades e exigências estabelecidas neste instrumento:

GRUPO	ITEM	DESCRIÇÃO/ESPECIFICAÇÃO	UNID.	QTDE	Valor estimado
01	01	**Aquisição e renovação de Antivírus** • Licenças de uso; • Solução de proteção de estações (computadores, notebooks, servidores); • Manutenção e suporte por 3 (três) anos • Quantitativo a ser renovado 1.200 (um mil e duzentas) • Quantitativo de novas Aquisições 1.800 (um mil e oitocentas)	Unid.	3000	R$ 142.760,00
	02	• **Treinamento para 10 Servidores do DTI.**	Unid.	10	R$ 26.000,00

2. JUSTIFICATIVA DA AQUISIÇÃO

2.1. O IFS conta com uma complexa estrutura computacional que garante o cumprimento de sua missão institucional e demanda dos gestores do segmento de tecnologia da informação e comunicação, especial atenção ao ambiente tecnológico em um nível que propicie o bom desempenho das atividades de seu corpo funcional.

2.2. Ao longo dos anos o IFS tem investido em recursos de tecnologia da informação e comunicação, de forma a assegurar o desempenho de suas atividades institucionais, possibilitando o tratamento de um grande e variado conjunto de informações.

2.3. A evolução da complexidade de demandas e soluções inerentes às atividades institucionais do IFS exige uma adequação e constante atualização das medidas que visam proteger e assegurar a qualidade e desempenho dos serviços prestados.

2.4. De acordo com a norma internacional ISO IEC 27001:2006, que trata da certificação para Sistemas de Gestão de Segurança de Informação e apresenta entre seus conceitos fundamentais os três atributos básicos da informação: confidencialidade, integridade e disponibilidade, é necessário que este centro, no exercício de suas atribuições institucionais promova e mantenha ações que permitam o IFS identificar, analisar e qualificar riscos que possam comprometer tais atributos.

2.5. Em decorrência disso, é fundamental a definição de estratégias que unifiquem os propósitos desses pilares da segurança da informação.

2.6. Dentre as medidas de segurança que garantem a proteção e a preservação das informações da instituição, destaca-se a utilização de uma ferramenta de detecção e de prevenção de contaminações ou ataques de programas maliciosos na rede do IFS.

2.7. Esse mecanismo visa manter todo o ambiente computacional protegido contra contaminações por vírus provenientes de mídias removíveis como pendrives ou discos rígidos portáteis, envio e recebimento de mensagens de correio eletrônico, acesso das estações de trabalho à internet e acesso por meio de notebooks e outros dispositivos móveis similares a recursos da rede corporativa do IFS.

2.8. Atualmente, a solução de antivírus é composta de interface centralizada de gerenciamento – EPO e software instalado nas estações de trabalho e computadores servidores do IFS, totalizando cerca de 1200 (um mil e duzentas) licenças de uso.

2.9. A interface de gerenciamento é responsável por gerenciar os serviços de varredura e bloqueio de falhas de segurança no parque computacional da instituição, além de controlar e manter atualizadas as estações de trabalho que possuem o software instalado.

2.10. O quantitativo da solução atual não contempla todos os computadores (estações de trabalho e servidores) de todos os Campi, estabelecendo assim pontos de vulnerabilidade a contaminações ou ataques de vírus, implicando em riscos à segurança dos serviços de tecnologia da informação e comunicação, tais como correio eletrônico, servidores de arquivos, acesso à internet, serviços de impressão e sistemas corporativos.

2.11. No processo de análise da viabilidade de substituição completa da solução atual por outra disponível no mercado verificou-se que tal processo implicaria em realizar a mudança das licenças de antivírus em todas as estações de trabalho e computadores servidores que fazem uso deste serviço, além de modificar a forma de gerenciamento, operação e monitoramento de falhas e ocorrência e tratamento de problemas.

2.12. Ademais, um processo de migração deste tipo de solução apresenta alto grau de complexidade e demanda tempo considerável de execução, tendo em vista a quantidade de computadores utilizados pela instituição, além da possibilidade de desencadear problemas na implantação local, e aumentar, de forma preponderante, os riscos de operação do serviço. A ocorrência de falhas na solução poderiam vir a causar impactos significativos na disponibilidade, performance e continuidade dos serviços, além de instabilidade nos aplicativos instalados nas estações de trabalho d o IFS.

2.13. A mudança completa da solução além de representar um considerável risco de instabilidade operacional, demandaria custos diretos e indiretos. Dentre os custos diretos citamos a substituição das licenças nos equipamentos, o próprio processo de migração, a substituição da interface central de gerenciamento e a transferência de tecnologia para que a equipe técnica pudesse absorver e se capacitar a gerenciar a nova solução. Dentre os custos indiretos citamos os impactos nos serviços de Tecnologia da Informação e Comunicação – TIC - decorrentes das interrupções em função da execução do processo de instalação e de configuração da nova solução, impactos nas rotinas operacionais dos usuários e nos projetos, haja vista a necessidade de dedicação exclusiva de parte da equipe de infraestrutura e suporte nas atividades de migração.

2.14. Ante o exposto, chegou-se à conclusão de que a manutenção da solução atual com aquisição de licenças complementares e renovação dos serviços de suporte técnico, manutenção e atualização de licenças por 36 meses se apresentam como a alternativa mais segura e adequada à garantia e evolução da confiabilidade, disponibilidade e segurança dos serviços de TIC utilizados na instituição. Além disso, mitigam-se os riscos que a existência de equipamentos não configurados com programa de antivírus trazem a uma rede corporativa complexa e fundamental na sustentação dos projetos, programas e atividades finalísticas que compõem a missão institucional do IFS.

2.15. Assim, faz-se necessária a aquisição de 1.800 (um mil e oitocentas) licenças para esse grupo de equipamentos, incorporando-os ao gerenciador central da solução, além da renovação das 1200 (um mil e duzentas) licenças de uso adquiridas anteriormente para que estas sejam igualmente cobertas por 36 (trinta e seis) meses pelo serviço de suporte técnico, garantindo a todo o ambiente do IFS acesso às atualizações diárias de vacinas, versões do produto e de novos módulos, com suporte técnico especializado quando da ocorrência de epidemias de vírus ou falhas no funcionamento da solução e seus componentes.

3. ESPECIFICAÇÕES

3.1. Especificação detalhada.

ITEM	Descrição do objeto
01	**LICENÇA DE USO SOFTWARE ANTIVÍRUS KASPERSKY BUSINESS SPACE SECURITY POR 36 MESES, com treinamento para 10 servidores:** **REQUISITOS MÍNIMOS:** **1. Servidor de Administração e Console Administrativa** 1.1. Compatibilidade: 1.1.1. Microsoft Windows Server 2003 ou superior 1.1.2. Microsoft Windows Server 2003 x64 ou superior 1.1.3. Microsoft Windows Server 2008 1.1.4. Microsoft Windows Server 2008 Core 1.1.5. Microsoft Windows Server 2008 x64 SP1 1.1.6. Microsoft Windows Server 2008 R2 1.1.7. Microsoft Windows Server 2008 R2 Core 1.1.8. Microsoft Windows XP Professional SP2 ou superior 1.1.9. Microsoft Windows XP Professional x64 1.1.10. Microsoft Windows Vista SP1 1.1.11. Microsoft Windows Vista x64 SP1 1.1.12. Microsoft Windows 7 1.1.13. Microsoft Windows 8 1.2. Características: 1.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC; 1.2.2. Capacidade de remover remotamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores; 1.2.3. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory; 1.2.4. Capacidade de instalar remotamente a solução de segurança em smartphones

Symbian, Windows Mobile e BlackBerry, utilizando estações como intermediadoras;

1.2.5. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux) protegidos pela solução antivírus;

1.2.6. Capacidade de gerenciar smartphones (tanto Symbian quanto Windows Mobile e BlackBerry) protegidos pela solução antivírus;

1.2.7. Deve gerenciar todos os módulos das soluções acima em uma única console.

1.2.8. Capacidade de gerar pacotes customizados (auto-executáveis) contendo a licença e configurações do produto;

1.2.9. Capacidade de atualizar os pacotes de instalação com as últimas vacinas, para que quando o pacote for utilizado em uma instalação já contenha as últimas vacinas lançadas;

1.2.10. Capacidade de fazer deployment (distribuição) remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

1.2.11. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

1.2.12. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção;

1.2.13. 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 serem adicionadas a proteção;

1.2.14. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

1.2.15. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

1.2.16. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

1.2.17. Deve fornecer as seguintes informações dos computadores;:

1.2.17.1. Se o antivírus está instalado;

1.2.17.2. Se o antivírus está iniciado;

1.2.17.3. Se o antivírus está atualizado;

1.2.17.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

1.2.17.5. Minutos/horas desde a última atualização de vacinas

1.2.17.6. Data e horário da última verificação executada na máquina;

1.2.17.7. Versão do antivírus instalado na máquina;

1.2.17.8. Se é necessário reiniciar o computador para aplicar mudanças;

1.2.17.9. Data e horário de quando a máquina foi ligada;

1.2.17.10. Quantidade de vírus encontrados (contador) na máquina;

1.2.17.11. Nome do computador;

1.2.17.12. Domínio ou grupo de trabalho do computador;

1.2.17.13. Data e horário da última atualização de vacinas;

1.2.17.14. Sistema operacional com ServicePack;

1.2.17.15. Quantidade de processadores;

1.2.17.16. Quantidade de memória RAM;

1.2.17.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

1.2.17.18. Endereço IP;

1.2.18. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

1.2.19. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

1.2.19.1. Mudança de gateway;

1.2.19.2. Mudança de subnet DNS;

1.2.19.3. Mudança de domínio;

1.2.19.4. Mudança de servidor DHCP;

1.2.19.5. Mudança de servidor DNS;

1.2.19.6. Mudança de servidor WINS;

1.2.19.7. Aparecimento de nova subnet;

1.2.20. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

1.2.21. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

1.2.22. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

1.2.23. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

1.2.24. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

1.2.25. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

1.2.26. Capacidade de gerar traps SNMP para monitoramento de eventos;

1.2.26.1. Capacidade de enviar mensagens via NETSEND para máquina específicas em caso de algum evento;

1.2.27. Capacidade de enviar emails para contas específicas em caso de algum evento;

1.2.28. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

1.2.29. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);

1.2.30. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).

1.2.31. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

1.2.32. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

1.2.33. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

2. Estações Windows

2.1. Compatibilidade:

2.1.1. Microsoft Windows 2000 Professional Service Pack 4 ou superior

2.1.2. Microsoft Windows XP Home Edition

2.1.3. Microsoft Windows XP Professional SP1 ou superior

2.1.4. Microsoft Windows XP Professional x64 Edition

2.1.5. Microsoft Windows Vista

2.1.6. Microsoft Windows Vista x64

2.1.7. Microsoft Windows 7 Professional/Enterprise/Ultimate

2.1.8. Microsoft Windows 7 Professional/Enterprise/Ultimate x64

2.1.9. Microsoft Windows 8

2.2. Características:

2.2.1. Deve prover as seguintes proteções:

2.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

2.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus)

2.2.1.3. Antivírus de Email (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos)

2.2.1.4. Anti-Spam (módulo de anti-spam pessoal)

2.2.1.5. Firewall com IDS

2.2.1.6. Auto-proteção (contra ataques aos serviços/processos do antivírus)

2.2.1.7. Controle de dispositivos externos

2.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independente do nível das ameaças encontradas no período (alta, média ou baixa).

2.2.4. Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;

2.2.5. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.2.6. 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 de acordo com o veredicto do antivírus, (ex: "Win32. Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.2.7. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

2.2.8. Possibilidade de desabilitar automaticamente varreduras agendadas quando o

computador estiver funcionando a partir de baterias (notebooks);

2.2.9. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

2.2.10. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;

2.2.11. Capacidade de verificar somente arquivos novos e alterados;

2.2.12. Capacidade de verificar objetos usando heurística;

2.2.13. Capacidade de agendar uma pausa na verificação;

2.2.14. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

2.2.15. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.2.15.1. Perguntar o que fazer, ou;

2.2.15.2. Bloquear acesso ao objeto;

2.2.15.2.1. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.15.2.2. Caso positivo de desinfecção:

2.2.15.2.2.1. Restaurar o objeto para uso;

2.2.15.2.3. Caso negativo de desinfecção:

2.2.15.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.16. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.2.17. Capacidade de verificar emails recebidos e enviados nos protocolos POP3, IMAP, NNTP, e SMTP, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);

2.2.18. Capacidade de verificar tráfego de ICQ e MSN contra vírus e links phishings;

2.2.19. Capacidade de verificar links inseridos em emails contra phishings;

2.2.20. Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Opera;

2.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

2.2.22. O antivírus de email, ao encontrar um objeto potencialmente perigoso, deve:

2.2.22.1. Perguntar o que fazer, ou;

2.2.22.2. Bloquear o email;

2.2.22.2.1. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.22.2.2. Caso positivo de desinfecção:

2.2.22.2.2.1. Restaurar o email para o usuário;

2.2.22.2.3. Caso negativo de desinfecção:

2.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.23. Caso o email conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

2.2.24. Possibilidade de verificar somente emails recebidos ou recebidos e enviados.

2.2.25. Capacidade de filtrar anexos de email, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador, com a possibilidade de restauração de um anexo deletado;

2.2.26. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;

2.2.27. Deve ter suporte total ao protocolo IPv6;

2.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e Email;

2.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

2.2.29.1. Perguntar o que fazer, ou;

2.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.2.29.3. Permitir acesso ao objeto;

2.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

2.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou;

2.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação. O administrador deve ter a capacidade de escolher quanto tempo de buffer o programa irá realizar.

2.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

2.2.32. 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.

2.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

2.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

2.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

2.2.36. Deve possuir módulo de bloqueio de Banners e Popups de propagandas não solicitadas, com opção de lista de exclusão;

2.2.37. Deve possuir módulo de proteção de atividades do modem, possibilitando a criação de uma lista de números que podem ser discados;

2.2.38. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

2.2.39. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

2.2.40. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.2.40.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.2.40.2. Filtragem por aplicação: onde o administrador poderá escolher qual aplicação terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.2.41. Deve possuir módulo de AntiSpam, que utilize tecnologias PDB (análise de cabeçalho), GSG (análise de elementos gráficos), tecnologia baseada no teorema de Bayes (http://pt.wikipedia.org/wiki/Filtro_bayesiano) além de White e Black Lists e algorítmo de reconhecimento de frases comuns de spams.

2.2.42. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

2.2.42.1. Dispositivos de comunicação USB (modems, telefones, etc.)

2.2.42.2. Impressoras USB

2.2.42.3. Dispositivos de armazenamento USB

2.2.42.4. Drives de CD\DVD-ROM

2.2.42.5. Drives de disquete

2.2.42.6. Dispositivos IEEE 1394 (Firewire)

2.2.42.7. Modems

2.2.42.8. Dispositivos PCMCIA

2.2.42.9. Dispositivos COM e LPT

2.2.42.10. Drives de fita

2.2.42.11. Dispositivos 1284 Dot4

2.2.42.12. Impressoras 1284 Dot4

2.2.42.13. Dispositivos Infravermelhos (IRDA)

2.2.42.14. Leitores de cartões (SD, MemoryStick, etc.)

2.2.42.15. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc)

2.2.42.16. Dispositivos Bluetooth

2.2.43. Deve ter capacidade para desabilitar o autoplay em todos os dispositivos (drives de cd, usb, rede, etc)

2.2.44. Deve ter capacidade para desabilitar o processamento de arquivos autorun.inf sem desabilitar o autoplay por completo.

3. Estações de trabalho Linux

3.1. Compatibilidade:

3.1.1. Plataforma 32-bits:

3.1.1.1. Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92)

3.1.1.2. Fedora 9 (kernel 2.6.25)

3.1.1.3. SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21)

3.1.1.4. openSUSE Linux 11.0 (kernel 2.6.25)

3.1.1.5. Debian GNU/Linux 4.0 r4 (kernel 2.6.24)

3.1.1.6. Mandriva Corporate Desktop 4 (kernel 2.6.12)

3.1.1.7. Ubuntu 8.04.1 Desktop Edition (kernel 2.6.25)

3.1.1.8. Linux XP Enterprise Desktop 2008 (2.6.25.10-47.3.lxp2008)

3.1.2. Plataforma 64-bits:

3.1.2.1. Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92)

3.1.2.2. Fedora 9 (kernel 2.6.25)

3.1.2.3. SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21)

3.1.2.4. openSUSE Linux 11.0 (kernel 2.6.25)

3.2. Características:

3.2.1. Deve prover as seguintes proteções:

3.2.1.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

3.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

3.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

3.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

3.2.2.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

3.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

3.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

3.2.3. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

3.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;

3.2.6. Capacidade de verificar objetos usando heurística;

3.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

3.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e

arquivos serão gravados

3.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

4. Servidores Windows

4.1. Compatibilidade:

4.1.1. Microsoft Windows 2000 Server Service Pack 4 + Update Rollup 1 ou superior

4.1.2. Microsoft Windows 2000 Advanced Server Service Pack 4 + Update Rollup 1 ou superior

4.1.3. Microsoft Windows Server 2003 Web/Standard/Enterprise/DataCenter Edition Service Pack 1 ou superior

4.1.4. Microsoft Windows Server 2003 Web/Standard/Enterprise/DataCenter Edition x64

4.1.5. Microsoft Windows Server 2003 R2 Standard/Enterprise/DataCenter Edition

4.1.6. Microsoft Windows Server 2003 R2 Standard/Enterprise/DataCenter Edition x64

4.1.7. Microsoft Windows Storage Server 2003 R2

4.1.8. Microsoft Windows Server 2008 Standard/Enterprise/DataCenter Edition

4.1.9. Microsoft Windows Server 2008 Standard/Enterprise/DataCenter Edition x64

4.1.10. Microsoft Windows Server 2008 Core Standard/Enterprise/DataCenter Edition

4.1.11. Microsoft Windows Server 2008 Core Standard/Enterprise/DataCenter Edition x64

4.1.12. Microsoft Terminal baseado em Windows 2000 Server

4.1.13. Microsoft Windows Small Business Server 2003

4.1.14. Microsoft Windows Small Business Server 2008

4.1.15. Windows Essential Business Server 2008

4.1.16. Microsoft Terminal baseado em Windows 2003 Server

4.1.17. Microsoft Terminal baseado em Windows 2008 Server

4.1.18. Citrix Metaframe XPe FR3;

4.1.19. Citrix Presentation Server 3.0

4.1.20. Citrix Presentation Server 4.0

4.1.21. Citrix Presentation Server 4.5

4.2. Características:

4.2.1. Deve prover as seguintes proteções:

4.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

4.2.1.2. Auto-proteção contra ataques aos serviços/processos do antivírus

4.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

4.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

4.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

4.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

4.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação)

4.2.4.3. Leitura de configurações

4.2.4.4. Modificação de configurações

4.2.4.5. Gerenciamento de Backup e Quarentena

4.2.4.6. Visualização de relatórios

4.2.4.7. Gerenciamento de relatórios

4.2.4.8. Gerenciamento de chaves de licença

4.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima)

4.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob-demanda e o número máximo de processos que podem ser executados no total.

4.2.6. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc.)

4.2.7. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS)

4.2.8. Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

4.2.9. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

4.2.10. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado nos servidor.

4.2.11. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

4.2.12. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

4.2.13. 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 de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

4.2.14. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

4.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;

4.2.16. Capacidade de verificar somente arquivos novos e alterados;

4.2.17. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto-descompressores, PST, arquivos compactados por compactadores binários, etc.)

4.2.18. Capacidade de verificar objetos usando heurística;

4.2.19. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

4.2.20. Capacidade de agendar uma pausa na verificação;

4.2.21. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

4.2.22. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

4.2.22.1. Perguntar o que fazer, ou;

4.2.22.2. Bloquear acesso ao objeto;

4.2.22.2.1. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

4.2.22.2.2. Caso positivo de desinfecção:

4.2.22.2.2.1. Restaurar o objeto para uso;

4.2.22.2.3. Caso negativo de desinfecção:

4.2.22.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

4.2.23. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

4.2.24. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena

4.2.25. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

4.2.26. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

5. Servidores Linux

5.1. Compatibilidade:

5.1.1. Plataforma 32-bits:

5.1.1.1. Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92)

5.1.1.2. Fedora 9 (kernel 2.6.25)

5.1.1.3. SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21)

5.1.1.4. Novel Open Enterprise Server 2 (kernel 2.6.16.46-0.12)

5.1.1.5. OpenSUSE Linux 11.0 (kernel 2.6.25)

5.1.1.6. Debian GNU/Linux 4.0 r4 (kernel 2.6.24)

5.1.1.7. Mandriva Corporate Server 4 (kernel 2.6.12)

5.1.1.8. Ubuntu 8.04.1 Server Edition (kernel 2.6.25)

5.1.2. Plataforma 64-bits:

5.1.2.1. Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92)

5.1.2.2. Fedora 9 (kernel 2.6.25)

5.1.2.3. SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21)

5.1.2.4. openSUSE Linux 11.0 (kernel 2.6.25)

5.2. Características:

5.2.1. Deve prover as seguintes proteções:

5.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan,

antimalware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

5.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

5.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

5.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

5.2.2.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

5.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

5.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

5.2.3. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

5.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

5.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;

5.2.6. Capacidade de verificar objetos usando heurística;

5.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena

5.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

5.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

6. Servidores Novell Netware:

6.1. Compatibilidade:

6.1.1. Novell Netware 5.x Support Pack 6 ou superior

6.1.2. Novell Netware 6.0 Support Pack 3 ou superior

6.1.3. Novell Netware 6.5

6.2. Características:

6.2.1. Deve possuir proteção em tempo real para arquivos acessados, criados ou modificados;

6.2.2. Deve possuir verificação manual e agendada de acordo com a configuração do administrador;

6.2.3. Capacidade de realizar update de maneira automática via internet ou LAN;

6.2.4. Capacidade de fazer um rollback das vacinas;

6.2.5. Capacidade de mover arquivos suspeitos ou infectados para área de quarentena;

6.2.6. Capacidade de criar logs detalhados e salvar resultados das verificações agendadas;

6.2.7. Capacidade de salvar um backup de todos os objetos infectados e suspeitos tratados;

6.2.8. Capacidade de notificar o administrador de varreduras concluídas e sobre objetos maliciosos encontrados no servidor, utilizando a rede Novell ou email;

RENOVAÇÃO LICENÇA DE USO SOFTWARE ANTIVÍRUS KASPERSKY BUSINESS SPACE SECURITY POR 36 MESES:

REQUISITOS MÍNIMOS:

1. Servidor de Administração e Console Administrativa

1.1. Compatibilidade:

1.1.1 Microsoft Windows Server 2003 ou superior

1.1.2 Microsoft Windows Server 2003 x64 ou superior

1.1.3 Microsoft Windows Server 2008

1.1.4 Microsoft Windows Server 2008 Core

1.1.5 Microsoft Windows Server 2008 x64 SP1

1.1.6 Microsoft Windows Server 2008 R2

1.1.7 Microsoft Windows Server 2008 R2 Core

1.1.8 Microsoft Windows XP Professional SP2 ou superior

1.1.9 Microsoft Windows XP Professional x64

1.1.10 Microsoft Windows Vista SP1

1.1.11 Microsoft Windows Vista x64 SP1

1.1.12 Microsoft Windows 7

1.1.13. Microsoft Windows 8

1.2 Características:

1.2.1 A console deve ser acessada via WEB (HTTPS) ou MMC;

1.2.2 Capacidade de remover remotamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

1.2.3 Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

1.2.4Capacidade de instalar remotamente a solução de segurança em smartphones Symbian, Windows Mobile e BlackBerry, utilizando estações como intermediadoras;

1.2.5 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux) protegidos pela solução antivírus;

1.2.6 Capacidade de gerenciar smartphones (tanto Symbian quanto Windows Mobile e BlackBerry) protegidos pela solução antivírus;

1.2.7 Deve gerenciar todos os módulos das soluções acima em uma única console.

1.2.8 Capacidade de gerar pacotes customizados (auto-executáveis) contendo a licença e configurações do produto;

1.2.9 Capacidade de atualizar os pacotes de instalação com as últimas vacinas, para que quando o pacote for utilizado em uma instalação já contenha as últimas vacinas lançadas;

1.2.10 Capacidade de fazer deployment (distribuição) remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

1.2.11 Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

2.2.12 Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção;

2.2.13 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 serem adicionadas a proteção;

2.2.14 Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou

grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

2.2.15Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

2.2.16 Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

2.2.17 Deve fornecer as seguintes informações dos computadores;

2.2.17.1 Se o antivírus está instalado;

2.2.17.2 Se o antivírus está iniciado;

2.2.17.3 Se o antivírus está atualizado;

2.2.17.4 Minutos/horas desde a última conexão da máquina com o servidor administrativo;

2.2.17.5 Minutos/horas desde a última atualização de vacinas

2.2.17.6 Data e horário da última verificação executada na máquina;

2.2.17.7 Versão do antivírus instalado na máquina;

2.2.17.8 Se é necessário reiniciar o computador para aplicar mudanças;

2.2.17.9 Data e horário de quando a máquina foi ligada;

2.2.17.10 Quantidade de vírus encontrados (contador) na máquina;

2.2.17.11 Nome do computador;

2.2.17.12 Domínio ou grupo de trabalho do computador;

2.2.17.13 Data e horário da última atualização de vacinas;

2.2.17.14 Sistema operacional com ServicePack;

2.2.17.15 Quantidade de processadores;

2.2.17.16 Quantidade de memória RAM;

2.2.17.17 Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

2.2.17.18 Endereço IP;

2.2.18 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

2.2.19 Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo,

baseado em regras de conexão como:

2.2.19.1 Mudança de gateway;

2.2.19.2 Mudança de subnet DNS;

2.2.19.3 Mudança de domínio;

1.2.19.4 Mudança de servidor DHCP;

1.2.19.5 Mudança de servidor DNS;

1.2.19.6 Mudança de servidor WINS;

1.2.19.7 Aparecimento de nova subnet;

1.2.20 Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

1.2.21 Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

1.2.22 Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

1.2.23 Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

1.2.24 Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

1.2.25 Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

1.2.26 Capacidade de gerar traps SNMP para monitoramento de eventos;

1.2.27 Capacidade de enviar mensagens via NETSEND para máquina específicas em caso de algum evento;

1.2.28 Capacidade de enviar emails para contas específicas em caso de algum evento;

1.2.29 Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

1.2.30 Deve possuir compatibilidade com Cisco Network Admission Control (NAC);

1.2.31 Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).

1.2.32Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em subnets diferentes do servidor;

1.2.33 Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

1.2.34 Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

2 Estações Windows –

2.1Compatibilidade:

2.1.1 Microsoft Windows 2000 Professional Service Pack 4 ou superior

2.1.2 Microsoft Windows XP Home Edition

2.1.3 Microsoft Windows XP Professional SP1 ou superior

2.1.4 Microsoft Windows XP Professional x64 Edition

2.1.5 Microsoft Windows Vista

2.1.6 Microsoft Windows Vista x64

2.1.7 Microsoft Windows 7 Professional/Enterprise/Ultimate

2.1.8 Microsoft Windows 7 Professional/Enterprise/Ultimate x64

2.1.9. Microsoft Windows 8

2.2 Características:

2.2.1 Deve prover as seguintes proteções:

2.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.2.1.2 Antivírus de Web (módulo para verificação de sites e downloads contra vírus)

2.2.1.3 Antivírus de Email (módulo para verificação de emails recebidos e enviados, assim como seus anexos)

2.2.1.4 Anti-Spam (módulo de anti-spam pessoal)

2.2.1.5 Firewall com IDS

2.2.1.6 Auto-proteção (contra ataques aos serviços/processos do antivírus)

2.2.1.7 Controle de dispositivos externos

2.2.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.2.3 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independente do nível das ameaças encontradas no período (alta, média ou baixa).

2.2.4 Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o

Firewall da solução;

2.2.5 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.2.6 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 de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.2.7 Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

2.2.8 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

2.2.9 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

2.2.10 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;

2.2.11 Capacidade de verificar somente arquivos novos e alterados;

2.2.12 Capacidade de verificar objetos usando heurística;

2.2.13 Capacidade de agendar uma pausa na verificação;

2.2.14 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

2.2.15 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.2.15.1 Perguntar o que fazer, ou;

2.2.15.2 Bloquear acesso ao objeto;

2.2.15.2.1 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.15.2.2 Caso positivo de desinfecção:

2.2.15.2.2.1 Restaurar o objeto para uso;

2.2.15.2.3 Caso negativo de desinfecção:

2.2.15.2.3.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.16 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.2.17 Capacidade de verificar emails recebidos e enviados nos protocolos POP3, IMAP, NNTP, e SMTP, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);

2.2.18 Capacidade de verificar tráfego de ICQ e MSN contra vírus e links phishings;

2.2.19 Capacidade de verificar links inseridos em emails contra phishings;

2.2.20 Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Opera;

2.2.21 Capacidade de verificação de corpo e anexos de emails usando heurística;

2.2.22 O antivírus de email, ao encontrar um objeto potencialmente perigoso, deve:

2.2.22.1 Perguntar o que fazer, ou;

2.2.22.2 Bloquear o email;

2.2.22.2.1 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.22.2.2 Caso positivo de desinfecção:

2.2.22.2.2.1 Restaurar o email para o usuário;

2.2.22.2.3 Caso negativo de desinfecção:

2.2.22.2.3.1 Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.23 Caso o email conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

2.2.24 Possibilidade de verificar somente emails recebidos ou recebidos e enviados.

2.2.25 Capacidade de filtrar anexos de email, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador, com a possibilidade de restauração de um anexo deletado;

2.2.26 Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;

2.2.27 Deve ter suporte total ao protocolo IPv6;

2.2.28 Capacidade de alterar as portas monitoradas pelos módulos de Web e Email;

2.2.29 Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

2.2.29.1 Perguntar o que fazer, ou;

2.2.29.2 Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.2.29.3 Permitir acesso ao objeto;

2.2.30 O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes,

sob escolha do administrador:

2.2.30.1 Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou;

2.2.30.2 Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação. O administrador deve ter a capacidade de escolher quanto tempo de buffer o programa irá realizar.

2.2.31 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

2.2.32 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.

2.2.33 Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

2.2.34 Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

2.2.35 Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

2.2.36 Deve possuir módulo de bloqueio de Banners e Popups de propagandas não-solicitadas, com opção de lista de exclusão;

2.2.37 Deve possuir módulo de proteção de atividades do modem, possibilitando a criação de uma lista de números que podem ser discados;

2.2.38 Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

2.2.39 Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

2.2.40 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.2.40.1Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.2.40.2 Filtragem por aplicação: onde o administrador poderá escolher qual aplicação terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.2.41 Deve possuir módulo de anti-spam, que utilize tecnologias PDB (análise de cabeçalho), GSG (análise de elementos gráficos), tecnologia baseada no teorema de Bayes (http://pt.wikipedia.org/wiki/Filtro_bayesiano) além de White e Black Lists e algorítmo de reconhecimento de frases comuns de spams.

2.2.42 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos

externos, no mínimo:

2.2.42.1 Dispositivos de comunicação USB (modems, telefones, etc.)

2.2.42.2 Impressoras USB

2.2.42.3 Dispositivos de armazenamento USB

2.2.42.4 Drives de CD\DVD-ROM

2.2.42.5 Drives de disquete

2.2.42.6 Dispositivos IEEE 1394 (Firewire)

2.2.42.7 Modems

2.2.42.8 Dispositivos PCMCIA

2.2.42.9 Dispositivos COM e LPT

2.2.42.10 Drives de fita

2.2.42.11 Dispositivos 1284 Dot4

2.2.42.12 Impressoras 1284 Dot4

2.2.42.13 Dispositivos Infravermelhos (IRDA)

2.2.42.14 Leitores de cartões (SD, MemoryStick, etc.)

2.2.42.15 Dispositivos de sincronização via ActiveSync (Windows CE, Windows Móbile, etc.)

2.2.42.16 Dispositivos Bluetooth

2.2.43 Deve ter capacidade para desabilitar o autoplay em todos os dispositivos (drives de cd, usb, rede, etc)

2.2.44 Deve ter capacidade para desabilitar o processamento de arquivos autorun.inf sem desabilitar o autoplay por completo.

3 Estações de trabalho Linux –

3.1 Compatibilidade:

3.1.1 Plataforma 32-bits:

3.1.1.1 Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92)

3.1.1.2 Fedora 9 (kernel 2.6.25)

3.1.1.3 SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21)

3.1.1.4 OpenSUSE Linux 11.0 (kernel 2.6.25)

3.1.1.5 Debian GNU/Linux 4.0 r4 (kernel 2.6.24)

3.1.1.6 Mandriva Corporate Desktop 4 (kernel 2.6.12)

3.1.1.7 Ubuntu 8.04.1 Desktop Edition (kernel 2.6.25)

3.1.1.8 Linux XP Enterprise Desktop 2008 (2.6.25.10-47.3.lxp2008)

3.1.2 Plataforma 64-bits:

3.1.2.1 Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92)

3.1.2.2 Fedora 9 (kernel 2.6.25)

3.1.2.3 SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21)

3.1.2.4 OpenSUSE Linux 11.0 (kernel 2.6.25)

3.2 Características:

3.2.1 Deve prover as seguintes proteções:

3.2.1.1 Antivírus de arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

3.2.1.2 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

3.2.2 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

3.2.2.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

3.2.2.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes; 3.2.2.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

3.2.2.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

3.2.3 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

3.2.4 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.2.5 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;

3.2.6 Capacidade de verificar objetos usando heurística;

3.2.7 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena

3.2.8 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

3.2.9Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

4Servidores Windows –

4.1Compatibilidade:

4.1.1 Microsoft Windows 2000 Server Service Pack 4 + Update Rollup 1 ou superior

4.1.2 Microsoft Windows 2000 Advanced Server Service Pack 4 + Update Rollup 1 ou superior

4.1.3 Microsoft Windows Server 2003 Web/Standard/Enterprise/DataCenter Edition Service Pack 1 ou superior

4.1.4 Microsoft Windows Server 2003 Web/Standard/Enterprise/DataCenter Edition x64

4.1.5 Microsoft Windows Server 2003 R2 Standard/Enterprise/DataCenter Edition

4.1.6 Microsoft Windows Server 2003 R2 Standard/Enterprise/DataCenter Edition x64

4.1.7 Microsoft Windows Storage Server 2003 R2

4.1.8 Microsoft Windows Server 2008 Standard/Enterprise/DataCenter Edition

4.1.9 Microsoft Windows Server 2008 Standard/Enterprise/DataCenter Edition x64

4.1.10 Microsoft Windows Server 2008 Core Standard/Enterprise/DataCenter Edition

4.1.11 Microsoft Windows Server 2008 Core Standard/Enterprise/DataCenter Edition x64

4.1.12 Microsoft Terminal baseado em Windows 2000 Server

4.1.13 Microsoft Windows Small Business Server 2003

4.1.14 Microsoft Windows Small Business Server 2008

4.1.15 Windows Essential Business Server 2008

4.1.16 Microsoft Terminal baseado em Windows 2003 Server

4.1.17 Microsoft Terminal baseado em Windows 2008 Server

4.1.18 Citrix Metaframe XPe FR3;

4.1.19 Citrix Presentation Server 3.0

4.1.20 Citrix Presentation Server 4.0

4.1.21 Citrix Presentation Server 4.5

4.2 Características:

4.2.1 Deve prover as seguintes proteções:

4.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

4.2.1.2 Auto-proteção contra ataques aos serviços/processos do antivírus

4.2.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

4.2.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

4.2.4 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

4.2.4.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

4.2.4.2 Gerenciamento de tarefa (criar ou excluir tarefas de verificação)

4.2.4.3 Leitura de configurações

4.2.4.4 Modificação de configurações

4.2.4.5 Gerenciamento de Backup e Quarentena

4.2.4.6 Visualização de relatórios

4.2.4.7 Gerenciamento de relatórios

4.2.4.8 Gerenciamento de chaves de licença

4.2.4.9 Gerenciamento de permissões (adicionar/excluir permissões acima)

4.2.5 Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

4.2.6 Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc.)

4.2.7 Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (Uninterruptible Power Supply – UPS)

4.2.8 Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

4.2.9 Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

4.2.10 Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado nos servidor.

4.2.11 Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

4.2.12 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

4.2.13 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 de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

4.2.14 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

4.2.15 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;

4.2.16 Capacidade de verificar somente arquivos novos e alterados;

4.2.17 Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto-descompressores, PST, arquivos compactados por compactadores binários, etc.)

4.2.18 Capacidade de verificar objetos usando heurística;

4.2.19 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

4.2.20 Capacidade de agendar uma pausa na verificação;

4.2.21 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

4.2.22 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

4.2.22.1 Perguntar o que fazer, ou;

4.2.22.2 Bloquear acesso ao objeto;

4.2.22.2.1 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

4.2.22.2.2 Caso positivo de desinfecção:

4.2.22.2.2.1 Restaurar o objeto para uso;

4.2.22.2.3 Caso negativo de desinfecção:

4.2.22.2.3.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

4.2.23 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

4.2.24 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em

quarentena

4.2.25 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

4.2.26 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

5 Servidores Linux –

5.1 Compatibilidade:

5.1.1 Plataforma 32-bits:

5.1.1.1 Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92)

5.1.1.2 Fedora 9 (kernel 2.6.25)

5.1.1.3 SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21)

5.1.1.4 Novel Open Enterprise Server 2 (kernel 2.6.16.46-0.12)

5.1.1.5 OpenSUSE Linux 11.0 (kernel 2.6.25)

5.1.1.6 Debian GNU/Linux 4.0 r4 (kernel 2.6.24)

5.1.1.7 Mandriva Corporate Server 4 (kernel 2.6.12)

5.1.1.8 Ubuntu 8.04.1 Server Edition (kernel 2.6.25)

5.1.2 Plataforma 64-bits:

5.1.2.1 Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92)

5.1.2.2 Fedora 9 (kernel 2.6.25)

5.1.2.3 SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21)

5.1.2.4 OpenSUSE Linux 11.0 (kernel 2.6.25)

5.2 Características:

5.2.1 Deve prover as seguintes proteções:

5.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

5.2.1.2 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

5.2.2 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

5.2.2.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

5.2.2.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um

reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

5.2.2.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

5.2.2.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

5.2.3 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

5.2.4 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

5.2.5 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;

5.2.6 Capacidade de verificar objetos usando heurística;

5.2.7 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena

5.2.8 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

5.2.9 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux)

6 Servidores Novell Netware:

6.1 Compatibilidade:

6.1.1 Novell Netware 5.x Support Pack 6 ou superior

6.1.2 Novell Netware 6.0 Support Pack 3 ou superior

6.1.3 Novell Netware 6.5

6.2 Características:

6.2.1 Deve possuir proteção em tempo real para arquivos acessados, criados ou modificados;
6.2.2 Deve possuir verificação manual e agendada de acordo com a configuração do administrador;

6.2.3 Capacidade de realizar update de maneira automática via internet ou LAN;

6.2.4 Capacidade de fazer um rollback das vacinas;

6.2.5 Capacidade de mover arquivos suspeitos ou infectados para área de quarentena;

6.2.6 Capacidade de criar logs detalhados e salvar resultados das verificações agendadas;

6.2.7 Capacidade de salvar um backup de todos os objetos infectados e suspeitos tratados;

6.2.8 Capacidade de notificar o administrador de varreduras concluídas e sobre objetos maliciosos encontrados no servidor, utilizando a rede Novell ou email;

Treinamento de utilização e configuração do SOFTWARE ANTIVÍRUS KASPERSKY BUSINESS SPACE SECURITY

Unidade I - Implementação

Capítulo 1 - Incidentes nas Organizações

Capítulo 2 - Instalação do Kaspersky Security Center

Capítulo 3 - Instalação nos computadores

Capítulo 4 - Gerenciamento da estrutura de computadores

Unidade II - Gerenciamento da Proteção

Capítulo 1 - Conceitos Básicos do Kaspersky EndPoint Security 8.0

Capítulo 2 - Sistema de Proteção de Arquivos

Capítulo 3 - Proteção da rede

Capítulo 4 - Defesa pró-ativa

Capítulo 5 - Diagnosticando ameaças

Capítulo 6 - Diagnósticos do status da proteção

Unidade III - Controle

Capítulo 1 - Controle de Aplicações

Capítulo 2 - Corrigindo vulnerabilidades

Capítulo 3 - Controle de dispositivos

Capítulo 4 - Controle WEB

Unidade IV - Manutenção

Capítulo 1 - Estatísticas e Relatórios

	Capítulo 2 - Atualizações Capítulo 3 - Gerenciamento de licenças Capítulo 4 - Interação com o usuário Capítulo 5 - Gerenciamento de computadores móveis Capítulo 6 - Backup e Restauração

3.2. Planilha descritiva.

ITEM	Descrição do objeto	Unid.	Qtd.	Valor Estimado
01	LICENÇA DE USO SOFTWARE ANTIVÍRUS KASPERSKY BUSINESS SPACE SECURITY POR **36 MESES**, para utilização em estações e servidores, com serviços de suporte técnico, manutenção e atualização de licenças.	Unid.	1.800	R$ 168.760,00
	RENOVAÇÃO LICENÇA DE USO SOFTWARE ANTIVÍRUS KASPERSKY BUSINESS SPACE SECURITY POR **36 MESES**, para utilização em estações e servidores, com serviços de suporte técnico, manutenção e atualização de licenças.	Unid.	1.200	
	Treinamento de utilização e configuração do SOFTWARE ANTIVÍRUS KASPERSKY BUSINESS SPACE SECURITY Unidade I - Implementação • Capítulo 1 - Incidentes nas Organizações • Capítulo 2 - Instalação do Kaspersky Security Center • Capítulo 3 - Instalação nos computadores • Capítulo 4 - Gerenciamento da estrutura de computadores Unidade II - Gerenciamento da Proteção • Capítulo 1 - Conceitos Básicos do Kaspersky EndPoint Security 8.0 • Capítulo 2 - Sistema de Proteção de Arquivos • Capítulo 3 - Proteção da rede • Capítulo 4 - Defesa pró-ativa • Capítulo 5 - Diagnosticando ameaças • Capítulo 6 - Diagnósticos do status da proteção Unidade III - Controle • Capítulo 1 - Controle de Aplicações • Capítulo 2 - Corrigindo vulnerabilidades • Capítulo 3 - Controle de dispositivos • Capítulo 4 - Controle WEB	Unid.	10	

	Unidade IV - Manutenção • Capítulo 1 - Estatísticas e Relatórios • Capítulo 2 - Atualizações • Capítulo 3 - Gerenciamento de licenças • Capítulo 4 - Interação com o usuário • Capítulo 5 - Gerenciamento de computadores móveis • Capítulo 6 - Backup e Restauração			

4. DA CLASSIFICAÇÃO DOS SERVIÇOS

4.1. O objeto deste termo de referência apresenta padrões de desempenho e qualidade que estão aqui descritos objetivamente por meio de especificações usuais praticadas no mercado, sendo, pois considerados bens comuns nos termos do Art. 1º da Lei 10.520 de 2002.

4.2. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto n° 2.271, de 1997, constituindo-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal do órgão licitante, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

4.3. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

5. INFORMAÇÕES RELEVANTES PARA O DIMENSIONAMENTO DA PROPOSTA

5.1. Serviço de suporte das licenças de *software*s adquiridas

5.1.1. O serviço de suporte técnico para 3.000 (três mil) licenças de uso do Software Antivírus – Kaspersky a ser prestado pelo período de 36 (trinta e seis) meses, contados a partir da data de aquisição, sem qualquer ônus adicional para o IFS;

5.1.2. Entende-se por manutenção corretiva aquela destinada a remover os defeitos apresentados pelos componentes de software da solução de antivírus, compreendendo também a atualização de versões dos componentes de software;

5.1.3. Entende-se por manutenção preventiva aquela destinada a atualizar os componentes do software e a realizar quaisquer operações que evitem uma parada parcial ou total da solução;

5.1.4. Entende-se por atendimento técnico aquele efetuado mediante atendimento realizado por telefone DDG (Discagem Direta Gratuita), e-mail e via web, de uso ilimitado telefônico ou no local (on site) para solução de problemas com os componentes de software ou apoio no tratamento de propagação de códigos

maliciosos, bem como para esclarecimentos de dúvidas sobre a configuração e a utilização da solução; Entende-se como atendimento via web, o registro e acompanhamento de solicitações feitas via navegador (browser);

5.1.5. O atendimento técnico (on site) será prestado nas instalações do IFS;

5.1.6. O atendimento e resolução de chamados deverão atender aos seguintes critérios:

5.1.6.1. SEVERIDADE 1:

5.1.6.1.1. Situação: esclarecimento de dúvidas em geral;

5.1.6.1.2. Atendimento: em até 2 (duas) horas por telefone ou e-mail, a contar do horário de abertura do chamado;

5.1.6.1.3. Resolução: em até 48 (quarenta e oito) horas, a contar do horário do início do atendimento.

5.1.6.2. SEVERIDADE 2:

5.1.6.2.1. Situação: ocorrência de códigos maliciosos que comprometam parcialmente a operação do ambiente computacional do IFS ou a solução tornou-se parcialmente indisponível em decorrência de falha ou de mau funcionamento;

5.1.6.2.2. Atendimento: em até 2 (duas) horas por telefone ou e-mail e até 4 (quatro) horas on-site, a contar do horário de abertura do chamado;

5.1.6.2.3. Resolução: em até 12 (doze) horas a contar do horário do início do atendimento.

5.1.6.3. SEVERIDADE 3:

5.1.6.3.1. Situação: ocorrência de códigos maliciosos que impeçam a realização de atividades críticas d o IFS ou a solução tornou-se totalmente indisponível em decorrência de falha ou de mau funcionamento;

5.1.6.3.2. Atendimento: em até 2 (duas) horas por telefone ou e-mail e até 4 (quatro) horas on-site, a contar do horário de abertura do chamado;

5.1.6.3.3. Resolução: em até 8 (oito) horas, a contar do horário do início do atendimento.

5.1.7. Para a prestação do serviço de suporte técnico, a empresa deverá manter central telefônica para abertura de chamados e atendimento técnico em português, na

modalidade 24x7 (vinte e quatro horas por sete dias por semana), sem ônus para o IFS;

5.1.8. A empresa deverá possuir recursos (e-mail, página web, central de atendimento telefônico, etc.) que permitam o IFS acompanhar o fluxo de um chamado desde a abertura até sua conclusão;

5.1.9. A empresa deverá fornecer, por sua exclusiva conta e sem ônus para o IFS, a atualização das versões e releases de todo o conjunto de softwares que compõe a solução, além do encaminhamento das mídias correspondentes.

5.1.10. A garantia e o suporte técnico devem obrigatoriamente prover atualização das versões dos softwares contemplados ou substituição dos mesmos por versões mais modernas, com no mínimo os mesmos requisitos da última versão substituída, em caso de descontinuidade dos produtos durante um período de 3 (três) anos;

5.1.11. O treinamento devera estar disponível para que o DTI marque, a qualquer tempo, o treinamento para os servidores, este treinamento poderá ser individual para que seja possível o bom andamento dos campi não prejudicando o suporte ao mesmo.

5.2. Serviços de treinamento de profissionais de tecnologia da informação

5.3. O treinamento será para 10 (dez) servidores indicados pelo DEPARTAMENTO DE TECNOLOGIA do IFS e o mesmo devera acontecer por um centro autorizado pela KASPERSKY. O treinamento poderá ser individual ou coletivo, pois dependera da disponibilidade do servidor para a data estabelecida

6. DA ENTREGA E SEU RECEBIMENTO

6.1. A entrega dos itens deverá ser realizada pelo licitante vencedor, no endereço: Reitoria, Av. Jorge Amado, 1551 – Loteamento Garcia – Bairro Jardins – CEP: 49025-330, Aracaju/SE, Divisão de Patrimônio, no prazo máximo de 20 (vinte) dias corridos, após a assinatura do contrato ou instrumento equivalente.

6.2. O recebimento das licenças será provisório, para posterior teste de conformidade e verificação das especificações técnicas deste Termo de Referência.

6.3. O IFS efetuará os testes de conformidade e verificação das licenças, em até 15 (quinze) dias após o recebimento provisório, para que seja configurado o recebimento definitivo e para que seja lavrado o termo de aceite momento no qual será recebido definitivamente o serviço.

6.3.1. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

6.4. O (s) material (ais) será (ao) recusado(s) se entregue(s) com as especificações técnicas diferentes das contidas neste Termo de Referência e na proposta.

6.5. A licitante vencedora terá o prazo de 72 (setenta e duas) horas corridas para providenciar a substituição da(s) licença(s) recusada(s) sem ônus para a Administração e sem prejuízo da aplicação de penalidade. Neste caso, o IFS terá novo prazo para testar a(s) licença(s).

6.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato.

7. DO REGIME DE EXECUÇÃO

7.1. O regime de execução será o de Empreitada por menor preço global.

8. OBRIGAÇÕES DA CONTRATANTE

8.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

8.2. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

8.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

8.4. Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas no Edital e seus anexos;

8.5. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura fornecida pela contratada.

9. OBRIGAÇÕES DA CONTRATADA

9.1. Proceder à entrega dos itens adjudicados, de conformidade com o quantitativo e as especificações constantes do item 1.1 do presente Termo de Referência e da sua proposta comercial.

9.2. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer as atualizações do software pelo período de 36 (trinta e seis) meses, na qualidade e quantidade especificadas neste Termo de Referência e em sua proposta.

9.3. Providenciar a troca, às suas expensas, dos materiais entregues com defeitos de fabricação e que não correspondam às especificações solicitadas, no prazo máximo de 03 (três) dias.

9.4. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrente de sua culpa ou dolo durante o período de entrega dos materiais, não implicando co-responsabilidade do Poder Público ou de seus agentes ou prepostos.

9.5. Responder por todo o ônus decorrente do transporte de embalagem, seguros, taxas, fretes e demais encargos que venham incidir na entrega dos materiais.

9.6. Lançar na nota fiscal as especificações dos materiais, de modo idêntico àquelas constantes do objeto do Edital de Pregão.

9.7. Não transferir a terceiros, total ou parcial, o fornecimento dos materiais sem a prévia e expressa anuência da Contratante.

9.8. A CONTRATADA deverá prover atualizações de todas as soluções fornecidas, inclusive upgrades de versões quando as antigas são descontinuadas durante o período de 36 (trinta e seis) meses sem ônus adicional para a CONTRATANTE, inclusive quanto à manutenção e suporte.

9.9. A CONTRATADA deverá prestar os serviços em até 20 (vinte) dias após a assinatura deste contrato compreendendo a entrega das licenças e o respectivo treinamento dos servidores.

10. DA SUBCONTRATAÇÃO

10.1. Não será admitida a subcontratação do objeto licitatório.

11. CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

11.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993, e do art. 6º do Decreto nº 2.271, de 1997.

11.2. O representante da Contratante deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato.

11.3. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

11.4. A execução dos contratos deverá ser acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam a mensuração dos aspectos mencionados no art. 34 da Instrução Normativa SLTI/MPOG nº 02, de 2008, quando for o caso.

11.5. O fiscal ou gestor do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do artigo 65 da Lei nº 8.666, de 1993.

11.6. A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca qualidade e forma de uso.

11.7. O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.

11.8. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 80 da Lei nº 8.666, de 1993.

11.9. As disposições previstas nesta cláusula não excluem o disposto no Anexo IV (Guia de Fiscalização dos Contratos de Terceirização) da Instrução Normativa SLTI/MPOG nº 02, de 2008, aplicável no que for pertinente à contratação.

11.10. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em co-responsabilidade da Contratante ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

12. DAS SANÇÕES ADMINISTRATIVAS

12.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

12.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

12.1.2. ensejar o retardamento da execução do objeto;

12.1.3. fraudar na execução do contrato;

12.1.4. comportar-se de modo inidôneo;

12.1.5. cometer fraude fiscal;

12.1.6. não mantiver a proposta.

12.2. A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

Ocorrência	Penalidades que poderão ser aplicadas
Recusar-se a assinar o instrumento de contrato.	1. Impedimento de licitar com o Instituto Federal de Sergipe pelo período de 2 (dois) anos. 2. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho.
Entregar o objeto fora do prazo estabelecido.	3. Multa de 1% (um por cento) por dia de atraso, aplicada sobre o valor do material não fornecido, limitada a 20 (vinte) dias. Após o vigésimo dia e a critério da Administração, poderá ser considerada inexecução total ou parcial do objeto.
Não efetuar a troca do objeto, quando notificado.	4. Impedimento de licitar com o Instituto Federal de Sergipe pelo período de 01 (um) ano. 5. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho.
Substituir o objeto fora do prazo estabelecido.	6. Multa de 1% (um por cento) por dia de atraso, aplicada sobre o valor do material não substituído, limitada a 20 (vinte) dias. Após o vigésimo dia e a critério da Administração, poderá ser considerada inexecução total ou parcial do objeto.
Deixar de entregar documentação exigida neste Edital.	7. Impedimento de licitar com o Instituo Federal de Sergipe pelo período de 1 (ano) ano. 8. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho/valor total estimado para o item ou lote.
Não mantiver a proposta ou desistir do lance.	9. Impedimento de licitar com o Instituo Federal de Sergipe pelo período de 01 (um) ano.

	10. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho.
Comportar-se de modo inidôneo.	11. Impedimento de licitar com o Instituo Federal de Sergipe pelo período de 02 (dois) anos. 12. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho.
Fizer declaração falsa.	13. Impedimento de licitar com a o Instituo Federal de Sergipe pelo período de 02 (dois) anos. 14. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho.
Apresentar documentação falsa.	15. Impedimento de licitar com a Administração Pública pelo período de 05 (cinco) anos. 16. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho. 17. Comunicar ao Ministério Público Federal.
Cometer fraude fiscal.	18. Impedimento de licitar com a Administração Pública pelo período de 05 (cinco) anos. 19. Multa de 10% (dez por cento) do valor do contrato/nota de empenho. 20. Comunicar ao Ministério Público Federal.
Deixar de executar qualquer obrigação pactuada ou prevista em lei e no edital do presente pregão eletrônico, em que não se comine outra penalidade.	21. Multa de 0,5% (meio por cento) por dia de atraso, aplicada sobre o valor do contrato/nota de empenho, limitada a 20 (vinte) dias. Após o vigésimo dia e a critério da Administração, poderá ser considerada inexecução total ou parcial do objeto.
Inexecução total.	22. Impedimento de licitar com o Instituo Federal de Sergipe pelo período de 05 (cinco) anos. 23. Multa de até 20% (vinte por cento) sobre o valor do contrato/nota de empenho.

Inexecução parcial do objeto.	24. Impedimento de licitar com o Instituo Federal de Sergipe pelo período de 02 (dois) ano. 25. Multa de até 10% (dez por cento) sobre o valor correspondente a parte não executada.

12.3. Também fica sujeita às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, a Contratada que:

12.3.1. tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

12.3.2. tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

12.3.3. demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

12.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

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

12.6. As penalidades serão obrigatoriamente registradas no SICAF.

Aracaju, 16 de julho de 2013.

_____

Toniclay Andrade Nogueira

Diretor de Tecnologia da Informação

Requisitante

APROVAÇÃO DO TERMO DE REFERÊNCIA

( ) Aprovado ( ) Não Aprovado

Data:___ / ___/ _____

_____
AILTON RIBEIRO DE OLIVEIRA
Reitor

ANEXO II

MODELOS DE DECLARAÇÕES
(Também disponíveis no sítio *www.comprasnet.gov.br*)

DECLARAÇÃO DE INEXISTÊNCIA DE FATO SUPERVENIENTE

A empresa_____, CNPJ nº. _____, declara sob as penas da lei, que até a presente data inexistem fatos impeditivos para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores.

_____ (local), _____ (data).

_____

(**representante legal do licitante, no âmbito da licitação, com identificação completa**)

DECLARAÇÃO DE MENOR

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

_____ (local), _____ (data).

_____

(**representante legal do licitante, no âmbito da licitação, com identificação completa**)

DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA

Pregão 19/2013

(**Identificação completa do representante da licitante – nome completo, CPF, RG e endereço completo**), como representante devidamente constituído de (**Identificação completa da licitante ou do Consórcio**) doravante denominado "licitante", para fins do disposto no **item 5.3.5** do **Edital 19/2013**, declara, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

a) a proposta apresentada para participar do **Pregão 19/2013** foi elaborada de maneira independente **pelo Licitante**, e o conteúdo da proposta não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato da do **Pregão 19/2013 do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe**, por qualquer meio ou por qualquer pessoa;

b) a intenção de apresentar a proposta elaborada para participar do **Pregão 19/2013 do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe,** não foi informada, discutida ou recebida de qualquer outro participante potencial ou de fato do **Pregão 19/2013**, por qualquer meio ou por qualquer pessoa;

c) que não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do **Pregão 19/2013** quanto a participar ou não da referida licitação;

d) que o conteúdo da proposta apresentada para participar do **Pregão 19/2013** não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro participante potencial ou de fato do **Pregão 19/2013** antes da adjudicação do objeto da referida licitação;

e) que o conteúdo da proposta apresentada para participar do **Pregão 19/2013** não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer integrante do **Instituto Federal de Educação, Ciência e Tecnologia de Sergipe** antes da abertura oficial das propostas; e

f) que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

_____, em _____ de _____ de _____

_____

(representante legal do licitante, no âmbito da licitação, com identificação completa)

ANEXO III – MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

INSERIR O TIMBRE DA EMPRESA CONTENDO SEU CNPJ E DADOS CADASTRAIS

Declaramos, sob as penas da lei, na qualidade de proponente do procedimento licitatório, sob a modalidade Pregão Eletrônico n.º 19/2013, cujo objeto é a aquisição, renovação e treinamento no uso de licenças de software de antivírus, que atendemos aos critérios de sustentabilidade ambiental, respeitando as normas de proteção ao meio ambiente, conforme estabelece a Instrução Normativa nº 01, de 19 de janeiro de 2010, nos casos em que a referida instrução se aplicar ao objeto.

Por ser a expressão da verdade, firmamos o presente.

Aracaju, _____ de _____ de 2013.

_____

Nome:
RG/CPF:
Cargo:

ANEXO IV – MODELO DE PROPOSTA DE PREÇOS

Ao
Instituto Federal de Educação, Ciência e Tecnologia de Sergipe
Pregão Eletrônico nº 19/2013 – Pregoeiro Agnaldo dos Santos
Processo: 23060.003025/2012-06

Razão social da empresa: XXXXXXXX
CNPJ: XXXX
Endereço: XXXXX
Telefone: (XX) xxxx-xxxx [**Ramal**: xxxx] – **Fax**: (XX) xxxx-xxxx – **Celular**: (XX) xxxx-xxxx
Email: xxxx@xxxx.com.br
Banco: XXXX; **Agência**: XXXX; **C/C**: XXXX
Representante da empresa: Nome _____; **Telefone**: xxxx-xxxx; **Email**: xxxx@xxxx.com.br

ITEM	DESCRIÇÃO DETALHADA	UND	QTD	Valor Total
01	.....	....	.....	R$ .....
02	.....	....	.....	R$ .....

VALIDADE DA PROPOSTA:	60 dias	GARANTIA/VALIDADE:	
PRAZO DE ENTREGA:	20 dias		

DECLARAMOS QUE NOS NOSSOS PREÇOS COTADOS ESTÃO INCLUÍDAS TODAS AS DESPESAS DIRETAS E INDIRETAS, FRETE, TRIBUTOS, TAXA DE ADMINISTRAÇÃO, ENCARGOS SOCIAIS, TRABALHISTAS, TRANSPORTE E SEGURO ATÉ O DESTINO, LUCRO E DEMAIS ENCARGOS DE QUALQUER NATUREZA NECESSÁRIOS AO CUMPRIMENTO INTEGRAL DO OBJETO DESTE EDITAL E SEUS ANEXOS, NADA MAIS SENDO VÁLIDO PLEITEAR A ESSE TÍTULO.

_____

Assinatura
CPF nº
RG nº

ANEXO V – MINUTA DE CONTRATO

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº 19/2013, QUE FAZEM ENTRE SI O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE E A EMPRESA .....

O **Instituto Federal de Educação, Ciência e Tecnologia de Sergipe – IFS**, sediado na Av. Jorge Amado, 1551, Loteamento Garcia, Bairro Jardins, CEP: 49.025-330, Aracaju/SE, inscrito no CNPJ/MF sob o nº 10.728.444/0001-00, neste ato representado pelo Reitor Ailton Ribeiro de Oliveira, inscrito no CPF sob o nº 077.847.755-04 portador da Carteira de Identidade nº 215.250 – SSP/SE, doravante denominada CONTRATANTE, e o (a) ..... Inscrito (a) no CNPJ/MF sob o nº ....., sediado (a) na ....., em ..... doravante designada CONTRATADA, neste ato representado pelo (a) Sr.(a) ....., portador (a) da Carteira de Identidade nº ....., expedida pela (o) ....., e CPF nº ....., tendo em vista o que consta no Processo nº 23060.003025/2012-06 e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 5.450, de 31 de maio de 2005, do Decreto nº 2.271, de 7 de julho de 1997, do Decreto nº 3.555, de 08 de agosto de 2000, das Instruções Normativas SLTI/MPOG nº 2, de 30 de abril de 2008 e suas alterações, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão nº 19/2013, mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de serviços de **aquisição, renovação e treinamento no uso de licenças de software de antivírus** com garantia e prestação de suporte, que serão prestados nas condições estabelecidas no Termo de Referência, Anexo I do Edital.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo acima, e à proposta vencedora, independentemente de transcrição.

1.3. Objeto da contratação:

GRUPO	ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	Valor estimado
01	**01**	**Aquisição e renovação de Antivírus** • **Licenças de uso;** • **Solução de proteção de estações (computadores, notebooks, servidores);** • **Manutenção e suporte por 3 anos (2013 2014 e 2015);** • **Quantitativo a ser renovado 1.200 (um mil e duzentas);** • **Quantitativo de novas Aquisições 1.800 (um mil e oitocentas).**	
	02	**Treinamento para 10 Servidores do DTI.**	

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato é aquele fixado no Edital, com início na data de sua assinatura e encerramento em 36 (trinta e seis) meses a contar desta.

2.1.1. A CONTRATADA não tem direito subjetivo à prorrogação contratual.

2.2. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

3. CLÁUSULA TERCEIRA – PREÇO

3.1. O valor total estimado da contratação é de R$..... (.....).

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4. CLÁUSULA QUARTA – DO REGIME DE EXECUÇÃO

4.1. O regime de execução será o de Empreitada por menor preço global:

5. CLÁUSULA QUINTA – DOTAÇÃO ORÇAMENTÁRIA

5.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 20...., na classificação abaixo:

Gestão/Unidade: 158134

Fonte: 0112000000

Programa de Trabalho: 12363203120RL0028

Elemento de Despesa: 44.90.39.93

PI: A2992P0100P

5.2. No(s) exercício(s) seguinte(s), as despesas correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

6. CLÁUSULA SEXTA – PAGAMENTO

6.1. O pagamento será efetuado pela Contratante no prazo de 15 (quinze) dias, contados da apresentação da Nota Fiscal/Fatura contendo o detalhamento dos serviços executados e os materiais empregados.

6.1.1. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

6.2. A apresentação da Nota Fiscal/Fatura deverá ocorrer no prazo de 5 (cinco) dias, contado da data final do período de adimplemento da parcela da contratação a que aquela se referir.

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

6.3. O pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação aos serviços efetivamente prestados e aos materiais empregados.

6.4. O pagamento será efetuado através de ordem bancária, para crédito em banco, agência e conta-corrente indicados pela Contratada.

6.5. O pagamento será efetuado em parcela única compreendendo o valor total do presente contrato não sobrevindo obrigações futuras quaisquer.

6.6. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária.

6.7. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

6.7.1. A Contratada regularmente optante pelo Simples Nacional não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

6.8. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \qquad I = \frac{(6/100)}{365} \qquad I = 0{,}00016438$$

TX = Percentual da taxa anual = 6%.

7. CLÁUSULA SÉTIMA – REAJUSTE

7.1. O preço é fixo e irreajustável.

8. CLÁUSULA OITAVA – GARANTIA DE EXECUÇÃO

8.1. O adjudicatário, no prazo de 10 (dez) dias úteis, após a assinatura do Termo de Contrato, prestará garantia no valor correspondente a 5% (cinco por cento) do valor do Contrato, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 56 da Lei nº 8.666, de 1993, desde que cumpridas às obrigações contratuais.

8.2. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de mais de 3 (três) meses após o término da vigência contratual.

8.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

8.3.1. prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

8.3.2. prejuízo causados à Contratante ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

8.3.3. as multas moratórias e punitivas aplicadas pela Contratante à Contratada.

8.3.4. Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela CONTRATADA.

8.4. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, até o máximo de 2% (dois por cento).

8.5. A garantia em dinheiro deverá ser efetuada na Caixa Econômica Federal, em conta específica com correção monetária, em favor do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe.

8.6. A Contratante não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses:

8.6.1. caso fortuito ou força maior;

8.6.2. alteração, sem prévia anuência da seguradora, das obrigações contratuais;

8.6.3. descumprimento das obrigações pelo contratado decorrentes de atos ou fatos praticados pela Contratante;

8.6.4. atos ilícitos dolosos praticados por servidores da Contratante.

8.7. Cabe à própria Contratante apurar a isenção da responsabilidade prevista nas alíneas acima, não sendo a entidade garantidora parte no processo instaurado pela Contratante.

8.8. Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas neste item.

8.9. Será considerada extinta a garantia:

8.9.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

8.9.2. no prazo de 90 (noventa) após o término da vigência, caso a Contratante não comunique a ocorrência de sinistros.

9. CLÁUSULA NONA – CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

9.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993, e do art. 6º do Decreto nº 2.271, de 1997.

9.2. O representante da Contratante deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato.

9.3. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

9.4. A execução dos contratos deverá ser acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam a mensuração dos aspectos mencionados no art. 34 da Instrução Normativa SLTI/MPOG nº 02, de 2008, quando for o caso.

9.5. O fiscal ou gestor do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à

produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do artigo 65 da Lei nº 8.666, de 1993.

9.6. A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca qualidade e forma de uso.

9.7. O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.

9.8. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 80 da Lei nº 8.666, de 1993.

9.9. As disposições previstas nesta cláusula não excluem o disposto no Anexo IV (Guia de Fiscalização dos Contratos de Terceirização) da Instrução Normativa SLTI/MPOG nº 02, de 2008, aplicável no que for pertinente à contratação.

9.10. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em co-responsabilidade da Contratante ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

10. CLÁUSULA DÉCIMA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

10.1. Obrigações da CONTRATANTE:

10.1.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

10.1.2. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

10.1.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

10.1.4. Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas no Edital e seus anexos;

10.1.5. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura fornecida pela contratada.

10.2. Obrigações da CONTRATADA:

10.2.1. Proceder à entrega dos itens adjudicados, conforme o quantitativo e as especificações constantes nas cláusulas 01 e 03 do Termo de Referência e da sua proposta comercial;

10.2.2. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer as atualizações do software pelo período de 36 (trinta e seis) meses, na qualidade e quantidade especificadas neste Termo de Referência e em sua proposta;

10.2.3. Providenciar a troca, às suas expensas, dos materiais entregues com defeitos de fabricação e que não correspondam às especificações solicitadas, no prazo máximo de 03 dias;

10.2.4. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrente de sua culpa ou dolo durante o período de entrega dos materiais, não implicando co-responsabilidade do Poder Público ou de seus agentes ou prepostos;

10.2.5. Responder por todo o ônus decorrente do transporte de embalagem, seguros, taxas, fretes e demais encargos que venham incidir na entrega dos materiais;

10.2.6. Lançar na nota fiscal as especificações dos materiais, de modo idêntico àquelas constantes do objeto do Edital de Pregão;

10.2.7. Não transferir a terceiros, total ou parcial, o fornecimento dos materiais sem a prévia e expressa anuência da Contratante;

10.2.8. A CONTRATADA deverá prover atualizações de todas as soluções fornecidas, inclusive upgrades de versões quando as antigas são descontinuadas durante o período de 36 (trinta e seis) meses sem ônus adicional para a CONTRATANTE, inclusive quanto à manutenção e suporte;

10.2.9. A CONTRATADA deverá prestar os serviços em até 20 (vinte) dias após a assinatura deste contrato compreendendo a entrega das licenças e o respectivo treinamento dos servidores.

11. CLÁUSULA DÉCIMA PRIMEIRA – SANÇÕES ADMINISTRATIVAS.

11.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

11.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

11.1.2. ensejar o retardamento da execução do objeto;

11.1.3. fraudar na execução do contrato;

11.1.4. comportar-se de modo inidôneo;

11.1.5. cometer fraude fiscal;

11.1.6. não mantiver a proposta.

11.2. A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

Ocorrência	Penalidades que poderão ser aplicadas
Recusar-se a assinar o instrumento de contrato.	1. Impedimento de licitar com o Instituto Federal de Sergipe pelo período de 2 (dois) anos. 2. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho.
Entregar o objeto fora do prazo estabelecido.	3. Multa de 1% (um por cento) por dia de atraso, aplicada sobre o valor do material não fornecido, limitada a 20 (vinte) dias. Após o vigésimo dia e a critério da Administração, poderá ser considerada inexecução total ou parcial do objeto.
Não efetuar a troca do objeto, quando notificado.	4. Impedimento de licitar com o Instituto Federal de Sergipe pelo período de 01 (um) ano. 5. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho.
Substituir o objeto fora do prazo estabelecido.	6. Multa de 1% (um por cento) por dia de atraso, aplicada sobre o valor do material não substituído, limitada a 20 (vinte) dias. Após o vigésimo dia e a critério da Administração, poderá ser considerada inexecução total ou parcial do objeto.
Deixar de entregar documentação exigida neste Edital.	7. Impedimento de licitar com o Instituo Federal de Sergipe pelo período de 1 (ano) ano. 8. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho/valor total estimado para o item ou lote.
Não mantiver a proposta ou desistir do lance.	9. Impedimento de licitar com o Instituo Federal de Sergipe pelo período de 01 (um) ano. 10. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho.
Comportar-se de modo inidôneo.	11. Impedimento de licitar com o Instituo Federal de Sergipe pelo período de 02 (dois) anos. 12. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho.

Fizer declaração falsa.	13. Impedimento de licitar com a o Instituo Federal de Sergipe pelo período de 02 (dois) anos. 14. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho.
Apresentar documentação falsa.	15. Impedimento de licitar com a Administração Pública pelo período de 05 (cinco) anos. 16. Multa de até 10% (dez por cento) do valor do contrato/nota de empenho. 17. Comunicar ao Ministério Público Federal.
Cometer fraude fiscal.	18. Impedimento de licitar com a Administração Pública pelo período de 05 (cinco) anos. 19. Multa de 10% (dez por cento) do valor do contrato/nota de empenho. 20. Comunicar ao Ministério Público Federal.
Deixar de executar qualquer obrigação pactuada ou prevista em lei e no edital do presente pregão eletrônico, em que não se comine outra penalidade.	21. Multa de 0,5% (meio por cento) por dia de atraso, aplicada sobre o valor do contrato/nota de empenho, limitada a 20 (vinte) dias. Após o vigésimo dia e a critério da Administração, poderá ser considerada inexecução total ou parcial do objeto.
Inexecução total.	22. Impedimento de licitar com o Instituo Federal de Sergipe pelo período de 05 (cinco) anos. 23. Multa de até 20% (vinte por cento) sobre o valor do contrato/nota de empenho.
Inexecução parcial do objeto.	24. Impedimento de licitar com o Instituo Federal de Sergipe pelo período de 02 (dois) ano. 25. Multa de até 10% (dez por cento) sobre o valor correspondente a parte não executada.

11.3. Também fica sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, a Contratada que:

11.3.1. tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

11.3.2. tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

11.3.3. demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

11.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada,

observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

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

11.6. As penalidades serão obrigatoriamente registradas no SICAF.

12. CLÁUSULA DÉCIMA SEGUNDA – RESCISÃO

12.1. O presente Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo do Edital.

12.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

12.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

12.4. O termo de rescisão, sempre que possível, deverá indicar:

12.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

12.4.2. Relação dos pagamentos já efetuados e ainda devidos;

12.4.3. Indenizações e multas.

13. CLÁUSULA DÉCIMA TERCEIRA – VEDAÇÕES

13.1. É vedado à CONTRATADA:

13.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

13.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

14. CLÁUSULA DÉCIMA QUARTA – ALTERAÇÕES

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

14.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

15. CLÁUSULA DÉCIMA QUINTA – PUBLICAÇÃO

15.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

16. CLÁUSULA DÉCIMA SEXTA – CASOS OMISSOS

16.1. Os casos omissos relacionados a este Contrato regular-se-ão pelos preceitos de direito público, aplicando-se-lhes, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado, notadamente as constantes nas Leis nº 10.406, de 10 de janeiro de 2002 e nº 8.078, de 11 de setembro de 1990, na forma dos arts. 54 e 55, inciso XII, da Lei nº 8.666, de 1993, bem como a legislação indicada no preâmbulo do presente Contrato.

17. CLÁUSULA DÉCIMA SÉTIMA – FORO

17.1. As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na Justiça Federal, no Foro da cidade de Aracaju, Seção Judiciária de Sergipe, com exclusão de qualquer outro, por mais privilegiado que seja.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

Aracaju - SE, ... de..... de 2013.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

CONTRATANTE

_____

Ailton Ribeiro de Oliveira
Reitor

_____

Responsável legal da CONTRATADA

TESTEMUNHAS:

_____ _____

CPF: CPF: