PROCESSO LICITATÓRIO: 13/2014

MODALIDADE: PREGÃO ELETRÔNICO Nº 07/2014

TIPO: MENOR PREÇO FINALIDADE: CONTRATAÇÃO

OBJETO: AQUISIÇÃO DE 300 (TREZENTAS) LICENÇAS DE SOFTWARE ANTIVÍRUS CORPORATIVO

SUMÁRIO

1. PREÂMBULO 2
2. OBJETO 4
3. DAS CONDIÇÕES DE PARTICIPAÇÃO 4
4. CREDENCIAMENTO NO SISTEMA E PARTICIPAÇÃO 5
5. RECEBIMENTO E ABERTURA DAS PROPOSTAS E FORMULAÇÃO DOS LANCES 6
6. PROPOSTA 7
7. DOS CRITÉRIOS DE JULGAMENTO 9
8. DA HABILITAÇÃO 10
9. JULGAMENTO 12
10. IMPUGNAÇÃO AO EDITAL E RECURSOS 12
11. HOMOLOGAÇÃO E CONTRATAÇÃO 13
12. PAGAMENTO 13
13. PENALIDADES 14
14. ENTREGA E RECEBIMENTO 14
15. ASSINATURA DO CONTRATO 15
16. DOTAÇÃO ORÇAMENTÁRIA 15
17. DISPOSIÇÕES FINAIS 15
ANEXO I - TERMO DE REFERÊNCIA 17
ANEXO II - DESCRIÇÃO DO OBJETO E ESPECIFICAÇÕES 18
ANEXO III – MINUTA DE CONTRATO 20
ANEXO IV – MODELO: DECLARAÇÃO - ART. 7º CF 365
ANEXO V – MODELO: DECLARAÇÃO ME/EPP 386
ANEXO VI – MODELO: DECLAR. INEXIST. DE FATO IMPEDITIVO 397
ANEXO VII – MODELO: PROPOSTA DE PREÇOS 408

PROCESSO LICITATÓRIO: 13/2014

MODALIDADE: PREGÃO ELETRÔNICO Nº 07/2014

TIPO: MENOR PREÇO FINALIDADE: CONTRATAÇÃO

OBJETO: AQUISIÇÃO DE 300 (TREZENTAS) LICENÇAS DE SOFTWARE ANTIVÍRUS CORPORATIVO.

1. PRÉAMBULO

PERÍODO DE ACOLHIMENTO DAS PROPOSTAS: Das 10h30 do dia 08/08/2014 até às 09h00 do dia 21/08/2014
DATA DE ABERTURA DAS PROPOSTAS: 21/08/2014
HORÁRIO DE ABERTURA DAS PROPOSTAS: 09h00
DATA DA DISPUTA DE PREÇOS: 21/08/2014
HORÁRIO DA DISPUTA DE PREÇOS: 10h30
TEMPO MÍNIMO DE DISPUTA: 05 minutos. Após 5 min. De disputa o pregoeiro poderá a qualquer momento acionar o tempo aleatório que pode variar de 00:00:01 (um segundo) à 00:30:00 (trinta minutos), determinado pelo sistema randômico da plataforma de licitações.

* **REFERÊNCIA DE TEMPO:** para todas as referências de tempo será considerado o horário de Brasília - DF.

1.1. O **CENTRO UNIVERSITÁRIO DE FRANCA – UNI-FACEF**, autarquia municipal (pessoa jurídica de direito público interno), com sede nesta cidade de Franca - SP, à Avenida Major Nicácio, nº 2433, São José, inscrita no CNPJ sob nº 47.987.136/0001-09, torna público para conhecimento dos interessados, que se acha aberta nesta unidade licitação na modalidade PREGÃO ELETRÔNICO nº **07**/2014, tipo **MENOR PREÇO POR LOTE**- Processo nº **13**/2013, cujo objeto é **AQUISIÇÃO DE 300 (TREZENTAS) LICENÇAS DE SOFTWARE ANTIVÍRUS CORPORATIVO**, que será regida pela seguinte legislação:

Lei Federal nº 10.520, de 17 de julho de 2002	Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências.
Decreto Federal nº 5.450, de 31 de maio de 2005	Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.
Decreto Federal 6.204/07	Regulamenta o tratamento favorecido, diferenciado e simplificado para as microempresas e empresas de pequeno porte nas contratações públicas de bens, serviços e obras, no âmbito da administração pública federal.
Decreto nº 3.555 de 08 de agosto de 2000	Aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.
Lei Complementar nº 123 de	Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno

14 de dezembro de 2006	Porte; altera dispositivos das Leis no 8.212 e 8.213, ambas de 24 de julho de 1991, da Consolidação das Leis do Trabalho - CLT, aprovada pelo Decreto-Lei no 5.452, de 1o de maio de 1943, da Lei no 10.189, de 14 de fevereiro de 2001, da Lei Complementar no 63, de 11 de janeiro de 1990; e revoga as Leis no 9.317, de 5 de dezembro de 1996, e 9.841, de 5 de outubro de 1999.
Lei Federal nº 8.666 e suas alterações.	Aplicada subsidiariamente no que couberem. Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.

1.2. As propostas deverão obedecer às especificações estabelecidas por este Edital e seus anexos, que dele fazem parte integrante.

1.3. O Pregão Eletrônico será realizado em sessão pública, por meio de sistema eletrônico de comunicação pela INTERNET. O sistema referido utiliza recursos de criptografia e de autenticação que asseguram condições adequadas de segurança em toda etapa do certame.

1.4. A informação dos dados para acesso deve ser feita na página inicial no sítio do Banco do Brasil S.A., www.bb.com.br, opção Licitações, ou diretamente em www.licitacoes-e.com.br.

1.5. A sessão pública de processamento da licitação será conduzida por pregoeiro, com suporte da Equipe de Apoio, membros da Comissão Permanente de Licitações designados, como consta nos autos do processo em epígrafe, os quais, juntamente com a autoridade competente do órgão promotor da licitação, formam o conjunto de operadores do sistema do Pregão Eletrônico.

1.6. O Pregão Eletrônico será realizado em sessão pública, por meio da *INTERNET*, mediante condições de segurança - criptografia e autenticação - em todas as suas fases.

1.6.1. O certame será realizado através da utilização do Portal Eletrônico do Banco do Brasil S.A. em sua página respectiva a processos licitatórios (www.licitacoes-e.com.br), conforme convênio de cooperação técnica celebrado entre o BB e o CENTRO UNIVERSITÁRIO DE FRANCA.

1.7. Integram o presente edital:

Anexo I – TERMO DE REFERÊNCIA;
Anexo II – DESCRIÇÃO DO OBJETO E ESPECIFICAÇÕES;
Anexo III – MINUTA DE CONTRATO;
Anexo IV – MODELO: DECLARAÇÃO - ART 7º CF;
Anexo V – MODELO: DECLARAÇÃO ME/EPP;
Anexo VI – MODELO: DECLARAÇÃO DE INEXISTÊNCIA DE FATO SUPERVENIENTE IMPEDITIVO;
Anexo VII – MODELO: PROPOSTA DE PREÇOS;

2. OBJETO

2.1. A presente licitação tem por objeto a **AQUISIÇÃO DE 300 (TREZENTAS) LICENÇAS DE SOFTWARE ANTIVÍRUS CORPORATIVO**, cuja adjudicação será feita pelo MENOR PREÇO POR LOTE ,conforme informações do Termo de Referência constante no **ANEXO I** e especificações constantes no **ANEXO II** , que integram este Edital.

2.2. Em caso de discordância existente entre as especificações deste objeto descritas na plataforma do Banco do Brasil e as especificações constantes deste Edital, prevalecerão as últimas.

3. DAS CONDIÇÕES DE PARTICIPAÇÃO

3.1. Poderão participar do certame as pessoas jurídicas do ramo de atividade pertinente ao objeto da licitação que atendam a todas as exigências constantes deste Edital e seus Anexos.

3.2. Não poderão participar da presente licitação

3.2.1. Os interessados suspensos de licitar com a Administração Municipal de Franca, cujo conceito abrange a administração direta e indireta, as entidades com personalidade jurídica de direito privado sob o seu controle e as fundações por ela instituída ou mantida, no prazo e nas condições do impedimento;

3.2.2. Empresa suspensa de contratar com o Uni-FACEF.

3.2.3. Os interessados que tenham sido declarados inidôneos pela Administração Municipal, Estadual ou Federal, o que abrange a administração direta e indireta, as entidades com personalidade jurídica de direito privado sob o seu controle e as fundações por ela instituída e mantida;

3.2.4. Os interessados que se encontrarem sob falência, concordata, concurso de credores, dissolução ou liquidação;

3.2.5. Empresas ou sociedades estrangeiras que não funcionam no país

3.2.6. Consórcio de empresa, qualquer que seja sua forma de constituição;

3.2.7. Empresa que esteja declarada inidônea para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade;

3.2.8. Empresa cujo objeto social não seja pertinente e compatível com o objeto deste Pregão.

3.3. A participação neste certame implica a aceitação de todas as condições estabelecidas neste instrumento convocatório.

4. CREDENCIAMENTO NO SISTEMA E PARTICIPAÇÃO

4.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e perante o sistema eletrônico provido pelo Banco do Brasil, por meio do sítio www.licitacoes-e.com.br. O cadastro é obrigatório e deve estar atualizado, sob pena de desclassificação.

4.2. O cadastramento no SICAF poderá ser realizado pelo interessado em qualquer unidade de cadastramento dos órgãos ou entidades da Presidência da República, dos Ministérios, das Autarquias e das Fundações que participam do Sistema Integrado de Serviços Gerais - SISG, localizada nas Unidades da Federação.

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

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

4.4. Os interessados deverão credenciar representantes, mediante a apresentação de procuração por instrumento público ou particular, com firma reconhecida, atribuindo poderes para formular lances de preços e praticar todos os demais atos e operações no sistema.

4.5. Em sendo sócio, proprietário, dirigente (ou assemelhado) da empresa proponente, deverá apresentar cópia do respectivo Estatuto ou Contrato Social, no qual estejam expressos seus poderes para exercer direitos e assumir obrigações em decorrência de tal investidura.

4.6. A chave de identificação e a senha terão validade de 01 (um) ano e poderão ser utilizadas em qualquer pregão eletrônico, salvo quando canceladas por solicitação do credenciado ou por iniciativa do Banco, devidamente justificado.

4.7. O credenciamento do fornecedor e de seu representante legal junto ao sistema eletrônico implica a responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes ao pregão eletrônico.

4.8. A participação no Pregão Eletrônico se dará por meio da digitação da senha pessoal e intransferível do representante credenciado e subseqüente encaminhamento da proposta de preços, exclusivamente por meio do sistema eletrônico, observados data e horário limite estabelecidos.

4.9. O encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital. O fornecedor será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

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

4.9.2. Por ocasião do envio da proposta, a licitante enquadrada como microempresa ou empresa de pequeno porte deverá declarar, em campo próprio do Sistema que atende aos requisitos do art. 3º da Lei Complementar nº 123/2006, para fazer jus aos benefícios previstos na referida Lei. Caso venha a ser declarada vencedora, ao ser intimada a apresentar proposta assinada e documentos de habilitação, dentre estes deverá conter a declaração constante no **ANEXO V.**

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

4.9.4. **Propostas que contiverem qualquer tipo de identificação da empresa (mesmo em seus anexos) serão automaticamente desclassificadas antes da abertura dos lances**.

4.10. Caberá ao fornecedor 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.

4.10.1. A comunicação entre o Pregoeiro e as licitantes ocorrerá mediante troca de mensagens, em campo próprio do sistema eletrônico.

4.11. Como requisito para participação neste Pregão, a licitante deverá declarar, em campo próprio do sistema eletrônico, que está ciente e concorda com as condições contidas no edital e seus anexos e que cumpre plenamente os requisitos de habilitação definidos neste Edital.

4.11.1. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e à proposta sujeitará a licitante às sanções previstas neste Edital e na legislação de regência.

5. RECEBIMENTO E ABERTURA DAS PROPOSTAS E FORMULAÇÃO DOS LANCES

5.1. As propostas serão recebidas até o horário previsto no preâmbulo deste edital, após o que terá início à sessão pública do pregão eletrônico, com a divulgação das propostas de preços recebidas, passando o Pregoeiro a avaliar sua aceitabilidade.

5.2. Aberta a etapa competitiva, os representantes dos fornecedores deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de registro e valor.

5.3. Só serão aceitos lances cujos valores forem inferiores ao último lance que tenha sido anteriormente registrado no sistema.

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

5.5. Durante o transcurso da sessão pública, os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances aos demais participantes.

5.6. 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, retomando o Pregoeiro, quando possível, sua atuação no certame, sem prejuízos dos atos realizados.

5.6.1. Quando a desconexão persistir por tempo superior a dez minutos, a sessão do Pregão Eletrônico será suspensa e terá reinício somente após comunicação expressa aos participantes, através da plataforma do Banco do Brasil (no campo DOCUMENTOS) divulgando data e hora da reabertura da sessão.

5.7. Depois de transcorridos 05 minutos da etapa de lances, o pregoeiro poderá a qualquer momento encerrar o **tempo normal** da disputa, mediante aviso de fechamento iminente dos lances emitido pelo sistema eletrônico, dando início ao período de tempo RANDÔMICO, podendo este variar **de 01 segundo até 30 minutos, aleatoriamente,** determinado automaticamente pelo sistema, findo o qual será automaticamente encerrada a recepção de lances.

5.8. Antes de anunciar o vencedor, o Pregoeiro poderá encaminhar pelo sistema eletrônico contra-proposta diretamente ao proponente que tenha apresentado o lance de menor preço, estando este na condição de arrematante, para que seja obtido preço melhor, bem como decidir sobre sua aceitação.

5.9. O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances ou, quando for o caso, após negociação e decisão pelo pregoeiro acerca da aceitação do lance de menor valor.

5.10. Caso não sejam apresentados lances, será verificada a conformidade entre a proposta de menor preço e valor estimado para a contratação.

5.11. **Erros de digitação de valores durante os lances serão de responsabilidade dos licitantes,** estando sujeitos ao cumprimento do valor ofertado ou às sanções cabíveis de acordo com análise da instituição.

6. PROPOSTA

6.1. A proposta deverá obedecer aos seguintes critérios:

6.1.1. Os preços deverão ser cotados em moeda corrente nacional, devendo o valor unitário proposto corresponder à unidade solicitada;

6.1.2. A licitante deverá, na forma expressa no sistema eletrônico, consignar os valores unitário e total e a descrição pormenorizada do produto ofertado para o item/lote o qual deseja enviar proposta especificando obrigatoriamente marca e modelo dos produtos.

6.1.3. Nos preços ofertados deverão já estar considerados e inclusos os tributos, fretes, tarifas e as **despesas decorrentes da execução do objeto.**

6.2. O prazo de validade da proposta é de 60 (sessenta) dias a contar da abertura da sessão pública estabelecida no preâmbulo deste Edital.

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

6.3. Prazo de Entrega: até 07 (sete) dias, após o recebimento do empenho.

6.4. É de inteira responsabilidade do licitante o preço e demais condições apresentadas, salvo se no momento da abertura da proposta for alegado erro, e aceito pelo Pregoeiro, será registrado em ata, devendo o item/lote ser desconsiderado da proposta.

6.5. A licitante vencedora do certame deverá disponibilizar as licenças em uma única parcela, atendendo às especificações constantes dos Anexos deste Edital, na plenitude de sua configuração.

6.6. Deverão ser especificados os prazos e condições de garantia para os produtos licitados, obedecendo a garantia mínima de 24 meses, referente à Assistência Técnica e atualizações disponíveis;

6.7. Os participantes desta licitação deverão prestar serviço de Assistência Técnica necessária ao perfeito funcionamento dos softwares durante o prazo de garantia, diretamente ou por empresa devidamente autorizada pelo fabricante, que será iniciado após a disponibilização dos mesmos.

6.8. A referida garantia deverá cobrir qualquer falha no Desempenho do Software, quando em condições normais de uso, bem como as atualizações do banco de dados do antivirus. Neste caso, todas as despesas serão custeadas pela adjudicada.

6.9. A Administração reserva-se o direito de recusar todo e qualquer software que não atenda às especificações deste Edital.

6.10. Os preços propostos serão considerados completos e abrangem todos os tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais) e qualquer despesa, acessória e/ou necessária, não especificada neste Edital.

6.11. No caso de discordância entre valores numéricos e por extenso, prevalecerão estes últimos e, entre preços unitários e totais, os primeiros.

6.12. Serão desclassificadas as propostas que conflitem com as normas deste Edital ou da legislação em vigor.

6.13. Serão rejeitadas as propostas que:

6.13.1. Estejam incompletas, isto é, não contenham informação(ões) suficiente(s) que permita(m) a perfeita identificação do objeto licitado;

6.13.2. Contiverem qualquer limitação ou condição substancialmente contrastante com o presente Edital, ou seja, manifestamente inexeqüíveis, por decisão do Pregoeiro.

6.14. O Uni-FACEF é considerado consumidor final, sendo que o licitante deverá obedecer ao texto fixado no art. 155, § 2º, VII, b, da Constituição Federal de 1988.

6.15. Qualquer elemento que possa identificar a licitante importa a desclassificação da proposta.

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

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

7. DOS CRITÉRIOS DE JULGAMENTO

7.1. Para julgamento, será adotado o critério de **MENOR PREÇO POR LOTE**, observados os prazos para fornecimento, as especificações técnicas, parâmetros mínimos de desempenho e qualidade e demais condições definidas neste Edital.

7.2. O Pregoeiro anunciará o licitante detentor da proposta ou lance de menor valor imediatamente após o encerramento da etapa de lances da sessão pública ou, quando for o caso, após negociação e decisão pelo Pregoeiro acerca da aceitação do lance de menor valor.

7.3. Se a proposta ou o lance de menor valor não for aceitável, o Pregoeiro examinará a proposta ou o lance subsequente, na ordem de classificação, verificando a sua aceitabilidade e procedendo à sua habilitação. Se for necessário, repetirá esse

procedimento, sucessivamente, até a apuração de uma proposta ou lance que atenda ao Edital.

7.4. Ocorrendo a situação a que se referem os itens 7.2 e 7.3 deste Edital, o Pregoeiro poderá negociar com o licitante para que seja obtido melhor preço.

7.5. Da sessão, o sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes.

8. DA HABILITAÇÃO

8.1. O licitante vencedor deverá apresentar a documentação original ou fotocópia autenticada no prazo máximo de **03 (três) dias úteis**, no DEPARTAMENTO DE COMPRAS do Centro Universitário de Franca, localizado à Avenida Major Nicácio, nº 2433, Bairro São José, Franca – SP CEP 14.401-135, informações pelo telefone (16) 3713-4688.

8.1.1. **Imediatamente após a conclusão dos lances** pelo sistema a equipe de apoio estará **recebendo VIA FAX ou E-MAIL a documentação digitalizada** exigida nos itens 8.3 a 8.5 deste edital, bem como a proposta formal assinada, e efetuando a consulta da situação cadastral da empresa vencedora dos lances no site do SICAF.

8.1.2. Se o licitante desatender as exigências habilitatórias, o pregoeiro examinará a proposta subsequente, verificando a sua aceitabilidade e procederá conforme a ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda ao edital.

8.2. Os documentos necessários à habilitação deverão ser apresentados em original ou por processo de cópia autenticada, na forma da lei. Fica dispensada a autenticação de certidões obtidas pela internet.

8.3. Para comprovação de REGULARIDADE FISCAL, (obs.: Serão aceitas *Certidões Positivas com Efeito de Negativas*) apresentar:

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ);

b) Prova de inscrição no Cadastro de Contribuintes Estadual e Municipal, se houver, relativo à sede ou ao domicílio da licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame;

c) Certidão de regularidade de débito com as Fazendas Estadual e Municipal, da sede ou do domicílio da licitante, expedida pelo órgão competente;

d) Certidão de regularidade de débito para com o Sistema de Seguridade Social (INSS);

e) Certidão de regularidade de débito para com o Fundo de Garantia por Tempo de Serviço (FGTS);

f) Certidão Conjunta Negativa de Débitos relativa a tributos federais e dívida ativa da União;

g) Certidão Negativa de Débitos Trabalhistas (CNDT), conforme lei nº 12.440/11.

8.4. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

h) Certidão negativa de falência ou concordata e recuperação judicial e extrajudicial expedida pelo distribuidor da sede da pessoa jurídica ou de execução patrimonial, expedida pelo distribuidor do domicílio da pessoa física;

8.5. OUTRAS COMPROVAÇÕES

Declarações abaixo relacionadas, subscritas por representante legal da licitante, elaborada em papel timbrado, sendo estas:

i) Declaração de cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal, conforme modelo constante no **ANEXO IV**.

j) Declaração de inexistência de fato superveniente impeditivo conforme modelo constante no **ANEXO VI**.

k) Documento de constituição da credenciada, conforme enquadramento abaixo:

- Registro empresarial na Junta Comercial, no caso de empresário individual;
- Ato constitutivo, estatuto ou contrato social e seus aditivos em vigor, devidamente registrado em se tratando de sociedades comerciais, e no caso de sociedade de ações, acompanhadas de documentos de eleição de seus administradores;
- Ato constitutivo devidamente registrado no Registro Civil de Pessoas Jurídicas tratando-se de sociedades não empresária acompanhado de prova da diretoria em exercício;
- Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo Órgão competente, quando a atividade assim o exigir.

k) Comprovante de cadastro no SICAF

8.6. Disposições gerais da habilitação:

8.6.1. É facultada às licitantes a não apresentação dos documentos de habilitação que constem do SICAF – Sistema de Cadastramento Unificado de Fornecedores, nos termos do art 4º, inciso XIV da Lei nº 10.520/02.

8.6.2. O registro cadastral (SICAF) não substitui os documentos relacionados nos subitens 8.4 e 8.5.

8.6.3. Na hipótese de não constar prazo de validade nas certidões apresentadas, a Administração aceitará como válidas as expedidas até 90 (noventa) dias imediatamente anteriores à data de apresentação das propostas.

8.7. Após a realização dos procedimentos relativos ao julgamento e ordenação das propostas, o Pregoeiro verificará a regularidade do cadastro e documentos da proponente vencedora.

8.8. Os documentos apresentados deverão ser, obrigatoriamente, da mesma sede, ou seja, se da matriz, todos da matriz, se de alguma filial, todos da mesma filial, com exceção dos documentos que são válidos para matriz e todas as filiais. Caso a empresa seja vencedora de um ou mais lotes, o contrato será celebrado com a sede que apresentou a documentação.

9. JULGAMENTO

9.1. Constatando o atendimento das exigências previstas no Edital, o licitante será declarado vencedor, sendo adjudicado o objeto da licitação e homologado o procedimento pela autoridade competente.

9.1.1. Havendo recurso, o pregoeiro apreciará os mesmos e, caso não reconsidere sua posição, caberá à autoridade competente a decisão em grau final

9.2. Após a habilitação, poderá a licitante ser desqualificada por motivo relacionado com a capacidade jurídica, regularidade fiscal, qualificação econômico-financeira, qualificação técnica e/ou inidoneidade, em razão de fatos supervenientes ou somente conhecidos após o julgamento.

10. IMPUGNAÇÃO AO EDITAL E RECURSOS

10.1. Impugnações ao ato convocatório do pregão serão recebidas até 02 (dois) dias úteis antes da data fixada para abertura do mesmo.

10.1.1. Caberá ao pregoeiro decidir sobre a impugnação, no prazo de 24 (vinte e quatro) horas.

10.1.2. Deferida a impugnação do ato convocatório, será designada nova data para realização do certame.

10.2. Ao final da disputa, o proponente que desejar recorrer contra decisões do Pregoeiro poderá fazê-lo, manifestando sua intenção com registro da síntese das suas razões em campo próprio aberto pelo sistema na parte inferior direita da tela, por meio da opção "RECURSO" que fica disponível por até 10 (dez) minutos, sendo-lhe facultado juntar memoriais no prazo de 3 (três) dias úteis. Os interessados ficam, desde logo, intimados a apresentar contrarrazões em igual prazo, que começará a correr do término do prazo do recorrente.

10.3. A falta de manifestação imediata e motivada do licitante importará a decadência do direito de recurso e a adjudicação ao vencedor do certame.

10.4. Os recursos contra decisões do pregoeiro não terão efeito suspensivo.

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

10.6. Não serão aceitas as impugnações e recursos apresentados fora do prazo legal, subscrito por representante não habilitado legalmente, ou não identificado no processo para responder pelo proponente.

11. HOMOLOGAÇÃO E CONTRATAÇÃO

11.1. Decididos os recursos e constatada a regularidade dos atos procedimentais, a autoridade competente adjudicará e homologará o objeto ao vencedor.

11.2. Como condição para a sua contratação o licitante vencedor deverá manter as mesmas condições de habilitação, prestar as informações solicitadas pela contratante, dentro dos prazos estipulados, bem como não transferir a outrem as obrigações decorrentes deste contrato.

11.3. A obrigação decorrente do fornecimento de bens será firmada entre a Administração e o Fornecedor, por meio de empenho, observando as condições estabelecidas neste Edital, seus anexos e na legislação vigente.

11.4. Quando o proponente vencedor, convocado dentro do prazo de validade da sua proposta, não celebrar a entrega ou não apresentar situação regular no ato do empenho deste, será convocado outro licitante, observada a ordem de classificação para celebrar o contrato, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

11.5. Este edital e todos os demais documentos que compõem seus anexos farão parte integrante do contrato.

12. PAGAMENTO

12.1. O objeto do presente pregão deverá ser entregue conforme especificações e prazos constantes nos ANEXOS I e II deste Edital, observando o seguinte:

12.1.1. Caso algum produto não corresponda ao exigido no instrumento convocatório, a contratada deverá providenciar no prazo máximo de 03 (três) dias, contados da data de notificação expedida pela contratante, a sua adequação, visando o atendimento das especificações, sem prejuízo da incidência das sanções previstas no instrumento convocatório, na Lei nº 8.666/93 e no Código de Defesa do Consumidor;

12.1.2. Os pagamentos serão efetuados mediante crédito em conta corrente devendo o fornecedor informar o número do banco, da agência e conta bancária, ou através de banco credenciado, a critério da Administração.

12.2. O prazo do pagamento devido pela Instituição é após 30 (trinta) dias, contados a partir da emissão do termo de recebimento definitivo do objeto licitado, mediante apresentação obrigatória da **nota fiscal eletrônica** devidamente atestada pelo setor requisitante.

13. PENALIDADES

13.1. O licitante que deixar de entregar quaisquer documentos exigidos no Edital ou apresentar documentação falsa para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta ou lance, não celebrar o contrato ou instrumento equivalente, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e contratar com a Administração Pública, pelo prazo de até 05 (cinco) anos, garantida a prévia defesa, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais.

13.2. O licitante sujeitar-se-á, ainda, às sanções de: advertência, multa e declaração de inidoneidade, sendo que as sanções de suspensão descritas no item anterior e declaração de inidoneidade poderão ser cumuladas com multa, sem prejuízo da rescisão contratual.

13.3. As multas poderão ser cumulativas, reiteradas e aplicadas em dobro, sempre que se repetir o motivo.

13.4. Ocorrendo atraso na execução/entrega do objeto contratado será aplicada multa moratória de **0,3%** (zero vírgula três por cento) por dia de atraso, até o limite de **20 %** (vinte por cento) sobre o valor total do contrato.

13.5. No descumprimento de quaisquer obrigações licitatórias/contratuais, poderá ser aplicada multa indenizatória de **10%** (dez por cento) do valor total do objeto licitado.

13.6. A multa, aplicada após regular processo administrativo, será descontada da(s) fatura(s), cobrada judicialmente ou extrajudicialmente, a critério da Instituição.

13.7. Da intenção de aplicação de quaisquer das penalidades previstas, será concedido prazo para defesa prévia de 5 (cinco) dias úteis a contar da notificação.

13.8. Da aplicação da sanção caberá recurso no prazo de 5 (cinco) dias úteis a contar da sua publicação.

13.9. As penalidades serão obrigatoriamente registradas, esgotada a fase recursal, no Cadastro de Fornecedores do Município, no caso de impedimento do direito de licitar e contratar, o licitante terá seu cadastro cancelado por igual período.

14. ENTREGA E RECEBIMENTO

14.1. Os softwares deverão conter todas as informações necessárias à perfeita caracterização dos mesmos, em Língua Portuguesa, como marca e demais especificações necessárias para a perfeita caracterização dos objetos.

14.2. As licenças e as instruções de instalação dos softwares deverão ser encaminhadas via e-mail (compras@facef.br) ou mídia digital ao Setor de Compras e Licitações do Uni-

FACEF, Unidade I, localizado na Avenida Major Nicácio, nº 2433 – Bairro São José – Franca/SP, CEP 14.401-135; em até 07 (sete) dias corridos após a formalização do pedido.

15. ASSINATURA DO CONTRATO

15.1. Após a homologação do resultado deste Pregão, a Administração do UNI-FACEF convocará a licitante vencedora, durante a validade da sua proposta, para assinatura do instrumento contratual, dentro do prazo de 3 (três) dias úteis, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital e no art. 81 da Lei n.º 8.666/1993.

15.2. O prazo para assinatura do contrato poderá ser prorrogado uma única vez, por igual período, quando solicitado pela licitante vencedora durante o seu transcurso, desde que ocorra motivo justificado e aceito pela Administração do UNI-FACEF.

15.3. A assinatura do contrato está condicionada à verificação da regularidade da habilitação parcial da licitante vencedora junto ao SICAF.

15.4. Poderá ser acrescentada ao contrato a ser assinado qualquer condição apresentada pela licitante vencedora em sua proposta, desde que seja pertinente e compatível com os termos deste Edital.

15.5. É facultado ao Pregoeiro, quando a convocada não assinar o contrato, no prazo e nas condições estabelecidos, convocar outra licitante, obedecida a ordem de classificação, para assiná-lo, após negociação, aceitação da proposta e comprovação dos requisitos de habilitação.

16. DOTAÇÃO ORÇAMENTÁRIA

16.1. As despesas decorrentes deste processo correrão à conta da dotação orçamentária do Uni-FACEF para o ano de 2014:

- 03.01.01 – Centro Universitário de Franca
- 3.3.90.39 – Outros Serviços de Terceiros – Pessoa Jurídica
- 3.3.90.39.11.001 – Locação de Softwares
- Ficha 12

16.2. A despesa com a aquisição de software antivirus de que trata o objeto é estimada em R$ 29.364,17 (vinte e nove mil trezentos e sessenta e quatro reais e dezessete centavos), conforme o orçamento estimativo disposto no Termo de Referência.

17. DISPOSIÇÕES FINAIS

17.1. As normas disciplinadoras desta licitação serão interpretadas em favor da ampliação da disputa, respeitada a igualdade de oportunidade entre os licitantes e desde que não comprometam o interesse público, a finalidade e a segurança da contratação.

17.2. É facultada ao Pregoeiro, ou à autoridade competente, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

17.3. A autoridade competente para determinar a contratação poderá revogar a licitação em face de razões de interesse público derivadas de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

17.4. A Administração reserva-se o direito de transferir o prazo para o recebimento e abertura das propostas descabendo, em tais casos, direito à indenização pelos licitantes.

17.5. A participação na presente licitação implica em concordância tácita, por parte do licitante, com todos os termos e condições deste Edital e das cláusulas contratuais já estabelecidas.

17.6. O resultado deste Pregão e os demais atos pertinentes a esta licitação, sujeitos à publicação, serão publicados no DOE.

17.7. Os casos omissos do presente Pregão serão solucionados pelo Pregoeiro.

17.8. Informações complementares, que visam obter maiores esclarecimentos sobre a presente licitação, serão prestadas pelo Pregoeiro via e-mail: compras@facef.br.

17.9. Para dirimir quaisquer questões decorrentes da licitação, não resolvidas na esfera administrativa, será competente o foro da Comarca de Franca, Estado de São Paulo, renunciando a outros por mais privilegiados que sejam.

Franca (SP), 05 de agosto de 2014.

_____	_____
Lucas Antônio Santos	*Prof. Dr. José Alfredo de Pádua Guerra*
Pregoeiro	*Pró-Reitor de Administração*

ANEXO I - TERMO DE REFERÊNCIA

PROCESSO LICITATÓRIO: 13/2014
MODALIDADE: PREGÃO ELETRÔNICO Nº 07/2014
TIPO: MENOR PREÇO FINALIDADE: CONTRATAÇÃO

Objeto		Aquisição de 300 licenças de software antivírus.
Valor total estimado da aquisição		**R$ 29.364,00 (vinte e nove mil trezentos e sessenta e quatro reais e dezessete centavos**)
Valor estimado unitário (por licença)	**Lote 01**	**R$ 97,18 (noventa e sete reais e dezoito centavos)**
Justificativa		Aquisição de 300 softwares antivírus com a finalidade de garantir a integridade, confiabilidade e segurança das informações contra ações de programas maléficos que ponham em risco a segurança, preservando os ativos corporativos de dados e protegendo o ambiente computacional do Uni-FACEF.
Prazos de entrega		Até 07 (sete) dias após o recebimento do Empenho
Prazo de garantia	**Lote 01**	O prazo de duração das licenças do software antivírus terá vigência de 24 (vinte e quatro) meses, sendo garantidas dento deste prazo todas as atualizações.
Classificação orçamentária		• 03.01.01 – Centro Universitário de Franca • 3.3.90.39 – Outros Serviços de Terceiros – Pessoa Jurídica • 3.3.90.39.11.001 – Locação de Softwares • Ficha 12
Local de entrega		Departamento de Licitações do Uni-FACEF, Unidade I, localizado na Avenida Major Nicácio, nº 2433 – Bairro São José – Franca/SP, CEP 14.401-135
Unidade fiscalizadora		Pró-Reitoria Administrativa

ANEXO II - DESCRIÇÃO DO OBJETO E ESPECIFICAÇÕES

PROCESSO LICITATÓRIO: 13/2014
MODALIDADE: PREGÃO ELETRÔNICO Nº 07/2014
TIPO: MENOR PREÇO FINALIDADE: CONTRATAÇÃO

Objeto: **AQUISIÇÃO DE 300 (TREZENTAS) LICENÇAS DE SOFTWARE ANTIVÍRUS CORPORATIVO.**

LOTE 01 – SOFTWARE ANTIVÍRUS CORPORATIVO

QUANTIDADE: 300 (trezentas)
UNIDADE: licença
DESCRIÇÃO: Software Antivírus Corporativo

Características e Especificações (Atributos Técnicos Mínimos Obrigatórios):

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 Server 2012
- 1.1.9. Microsoft Windows XP Professional SP2 ou superior
- 1.1.10. Microsoft Windows XP Professional x64
- 1.1.11. Microsoft Windows Vista SP1
- 1.1.12. Microsoft Windows Vista x64 SP1
- 1.1.13. Microsoft Windows 7
- 1.1.14. Microsoft Windows 7 x64
- 1.1.15. Microsoft Windows 8
- 1.1.16 Microsoft Windows 8 x64
- 1.1.17. Microsoft Windows 8.1
- 1.1.18 Microsoft Windows 8.1 x64

1.2. Características:
- 1.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
- 1.2.2. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
- 1.2.3. Capacidade de remover remotamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores, sem a necessidade da senha de remoção do atual antivírus;
- 1.2.4. 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;
- 1.2.5. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets Symbian, Windows Mobile, BlackBerry e Android, utilizando estações como intermediadoras;
- 1.2.6. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS;

1.2.7. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
1.2.8. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac OS X) protegidos pela solução antivírus;
1.2.9. Capacidade de gerenciar smartphones e tablets (tanto Symbian quanto Windows Mobile, BlackBerry, Android e iOS) protegidos pela solução antivírus;
1.2.10. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
1.2.11. 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;
1.2.12. Capacidade de fazer 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;
1.2.13. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
1.2.14. Capacidade de aplicar atualizações do Windows remotamente nas estações e servidores;
1.2.15. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
1.2.16. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção;
1.2.17. 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;
1.2.18. 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;
1.2.19. 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;
1.2.20. 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;
1.2.21. Deve fornecer as seguintes informações dos computadores:
1.2.21.1. Se o antivírus está instalado;
1.2.21.2. Se o antivírus está iniciado;
1.2.21.3. Se o antivírus está atualizado;
1.2.21.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
1.2.21.5. Minutos/horas desde a última atualização de vacinas;
1.2.21.6. Data e horário da última verificação executada na máquina;
1.2.21.7. Versão do antivírus instalado na máquina;
1.2.21.8. Se é necessário reiniciar o computador para aplicar mudanças;
1.2.21.9. Data e horário de quando a máquina foi ligada;
1.2.21.10. Quantidade de vírus encontrados (contador) na máquina;
1.2.21.11. Nome do computador;
1.2.21.12. Domínio ou grupo de trabalho do computador;
1.2.21.13. Data e horário da última atualização de vacinas;
1.2.21.14. Sistema operacional com Service Pack;
1.2.21.15. Quantidade de processadores;
1.2.21.16. Quantidade de memória RAM;
1.2.21.17. Usuário(s) logado(s) naquele momento, com informações de contato(caso disponíveis no Active Directory);
1.2.21.18. Endereço IP;
1.2.21.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.
1.2.21.20. Atualizações do Windows Updates instaladas
1.2.21.21.Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
1.2.21.22. Vulnerabilidades de aplicativos instalados na máquina;

1.2.22 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga altera-las;
1.2.23. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
1.2.23.1. Mudança de gateway;
1.2.23.2. Mudança de subnet DNS;
1.2.23.3. Mudança de domínio;
1.2.23.4. Mudança de servidor DHCP;
1.2.23.5. Mudança de servidor DNS;
1.2.23.6. Mudança de servidor WINS;
1.2.23.7. Aparecimento de nova subnet;
1.2.24.Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
1.2.25.Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
1.2.26.Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
1.2.27.Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
1.2.28. 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;
1.2.29. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
1.2.30. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
1.2.31. Capacidade de gerar traps SNMP para monitoramento de eventos;
1.2.32. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
1.2.33. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
1.2.34. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
1.2.35. Deve possuir documentação da estrutura do banco de dados para geração de
relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por
exemplo).
1.2.36. 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;
1.2.37. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
1.2.38. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
1.2.39. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.
1.2.40. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
1.2.41. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
1.2.42. Capacidade de diferenciar máquinas virtuais de máquinas físicas;

2. Estações Windows

2.1. Compatibilidade:
2.1.1. Microsoft Windows XP Professional SP3
2.1.2. Microsoft Windows Vista Business/Enterprise/Ultimate SP2
2.1.3. Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2
2.1.4. Microsoft Windows 7 Professional/Enterprise/Ultimate
2.1.5. Microsoft Windows 7 Professional/Enterprise/Ultimate x64
2.1.6. Microsoft Windows 8 Professional/Enterprise
2.1.7. Microsoft Windows 8 Professional/Enterprise x64

2.1.8. Microsoft Windows 8.1 Professional/Enterprise
2.1.9. Microsoft Windows 8.1 Professional/Enterprise x64
2.2. Características:
2.2.1. Deve prover as seguintes proteções:
2.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, 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 E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos)
2.2.1.4. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc)
2.2.1.5. Firewall com IDS
2.2.1.6. Autoproteção (contra ataques aos serviços/processos do antivírus)
2.2.1.7. Controle de dispositivos externos
2.2.1.8. Controle de acesso a sites por categoria
2.2.1.9. Controle de execução de aplicativos
2.2.1.10. Controle de vulnerabilidades do Windows e dos aplicativos instalados
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 independentemente 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 e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
2.2.18. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
2.2.19. Capacidade de verificar links inseridos em e-mails 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 e-mail, ao encontrar um objeto potencialmente perigoso, deve:
2.2.22.1. Perguntar o que fazer, ou;
2.2.22.2. Bloquear o e-mail;
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 e-mail 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 e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.
2.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.
2.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.
2.2.26. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (Java Script, 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 E-mail;
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.
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. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
2.2.37. 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.
2.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
2.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
2.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a

possibilidade de escolher quais portas e protocolos poderão ser utilizados.

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

2.2.39.1. Discos de armazenamento locais
2.2.39.2. Armazenamento removível
2.2.39.3. Impressoras
2.2.39.4. CD/DVD
2.2.39.5. Drives de disquete
2.2.39.6. Modems
2.2.39.7. Dispositivos de fita
2.2.39.8. Dispositivos multifuncionais
2.2.39.9. Leitores de smart card
2.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc)
2.2.39.11. Wi-Fi
2.2.39.12. Adaptadores de rede externos
2.2.39.13. Dispositivos MP3 ou smartphones
2.2.39.14. Dispositivos Bluetooth

2.2.40. Capacidade de liberar acesso a um dispositivo específico e usuários específico por um período de tempo específico, sem a necessidade de desabilitar a proteção, sem desabilitar o gerenciamento central ou de intervenção local do administrador na máquina do usuário.

2.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

2.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

2.2.43. Capacidade de configurar novos dispositivos por Class ID/Hardware ID 2.2.44. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário ou grupos de usuários e agendamento.

2.2.45. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc).

2.2.46. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

2.2.47. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.

2.2.48. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso a web.

2.2.49. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso a web.

3. Estações e Servidores Mac OS X

3.1. Compatibilidade:

3.1.1. Mac OS X 10.4.11 ou superior
3.1.2. Mac OS X Server 10.6
3.1.3. Mac OS X Server 10.7

3.2. Características:

3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti- malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

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

3.2.3. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;

3.2.4. Deve possuir suportes a notificações utilizando o Growl;

3.2.5. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos

usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

3.2.6. Capacidade de voltar para a base de dados de vacina anterior;

3.2.7. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

3.2.8. 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;

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

3.2.10. 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;

3.2.11. Capacidade de verificar somente arquivos novos e alterados;

3.2.12. Capacidade de verificar objetos usando heurística;

3.2.13. Capacidade de agendar uma pausa na verificação;

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

3.2.14.1. Perguntar o que fazer, ou;

3.2.14.2. Bloquear acesso ao objeto;

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

3.2.14.2.2. Caso positivo de desinfecção:

3.2.14.2.2.1. Restaurar o objeto para uso;

3.2.14.2.3. Caso negativo de desinfecção:

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

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

3.2.16. Capacidade de verificar arquivos de formato de e-mail;

3.2.17. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

3.2.18. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento;

4. Estações de trabalho Linux

4.1. Compatibilidade:

4.1.1. Plataforma 32-bits:

4.1.1.1. Canaima 3

4.1.1.2. Red Flag Desktop 6.0 SP2

4.1.1.3. Red Hat Enterprise Linux 5.8 Desktop

4.1.1.4. Red Hat Enterprise Linux 6.2 Desktop

4.1.1.5. Fedora 16

4.1.1.6. CentOS-6.2

4.1.1.7. SUSE Linux Enterprise Desktop 10 SP4

4.1.1.8. SUSE Linux Enterprise Desktop 11 SP2

4.1.1.9. openSUSE Linux 12.1

4.1.1.10. openSUSE Linux 12.2

4.1.1.11. Debian GNU/Linux 6.0.5

4.1.1.12. Mandriva Linux 2011

4.1.1.13. Ubuntu 10.04 LTS

4.1.1.14. Ubuntu 12.04 LTS

4.1.2. Plataforma 64-bits:

4.1.2.1. Canaima 3
4.1.2.2. Red Flag Desktop 6.0 SP2
4.1.2.3. Red Hat Enterprise Linux 5.8
4.1.2.4. Red Hat Enterprise Linux 6.2 Desktop
4.1.2.5. Fedora 16
4.1.2.6. CentOS-6.2
4.1.2.7. SUSE Linux Enterprise Desktop 10 SP4
4.1.2.8. SUSE Linux Enterprise Desktop 11 SP2
4.1.2.9. openSUSE Linux 12.1
4.1.2.10. openSUSE Linux 12.2
4.1.2.11. Debian GNU/Linux 6.0.5
4.1.2.12. Ubuntu 10.04 LTS
4.1.2.13. Ubuntu 12.04 LTS

4.2. Características:

4.2.1. Deve prover as seguintes proteções:

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

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

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

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

4.2.2.2. 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;

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

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

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

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

4.2.5. 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;

4.2.6. Capacidade de verificar objetos usando heurística;

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

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

4.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux). 5. Servidores Windows –

5. Servidores Windows

5.1. Compatibilidade:

5.1.1. Microsoft Windows Small Business Server 2011 Essentials/Standard x64
5.1.2. Microsoft Windows Server 2003 Standard/Enterprise SP2 x86/x64
5.1.3. Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 x86/x64
5.1.4. Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1 x86/x64
5.1.5. Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 x86/x64
5.1.6. Microsoft Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1
5.1.7. Microsoft Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1
5.1.8. Microsoft Windows Server 2012 Foundation/Essentials/Standard x64

5.1.9. Microsoft Windows Hyper-V Server 2008 R2 SP1
5.1.10. Microsoft Terminal baseado em Windows Server 2003
5.1.11. Microsoft Terminal baseado em Windows Server 2008
5.1.12. Microsoft Terminal baseado em Windows Server 2008 R2
5.1.13. Citrix Presentation Server 4.0 e 4.5
5.1.14. Citrix XenApp 4.5, 5.0 e 6.0

5.2. Características:
5.2.1. Deve prover as seguintes proteções:
5.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
5.2.1.2. Autoproteção contra ataques aos serviços/processos do antivírus
5.2.1.3. Firewall com IDS
5.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados
5.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
5.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
5.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
5.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação)
5.2.4.3. Leitura de configurações
5.2.4.4. Modificação de configurações
5.2.4.5. Gerenciamento de Backup e Quarentena
5.2.4.6. Visualização de relatórios
5.2.4.7. Gerenciamento de relatórios
5.2.4.8. Gerenciamento de chaves de licença
5.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima)
5.2.5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
5.2.5.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
5.2.5.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
5.2.6. 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.
5.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc)
5.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS)
5.2.9. Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
5.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.
5.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado nos servidor.
5.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.
5.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5.2.14. 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;
5.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
5.2.16. 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;
5.2.17. Capacidade de verificar somente arquivos novos e alterados;
5.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto-descompressores, .PST, arquivos compactados por compactadores binários, etc)
5.2.19. Capacidade de verificar objetos usando heurística;
5.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças; 5.2.21. Capacidade de agendar uma pausa na verificação;
5.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
5.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
5.2.23.1. Perguntar o que fazer, ou;
5.2.23.2. Bloquear acesso ao objeto;
5.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
5.2.23.2.2. Caso positivo de desinfecção:
5.2.23.2.2.1. Restaurar o objeto para uso;
5.2.23.2.3. Caso negativo de desinfecção:
5.2.23.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
5.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
5.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
5.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
5.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

6. Servidores Linux

6.1. Compatibilidade:
6.1.1. Plataforma 32-bits:
6.1.1.1. Canaima 3
6.1.1.2. Asianux Server 3 SP4
6.1.1.3. Asianux Server 4 SP1
6.1.1.4. Red Hat Enterprise Linux 6.2 Server;
6.1.1.5. Red Hat Enterprise Linux 5.8 Server
6.1.1.6. Fedora 16;
6.1.1.7. CentOS-6.2;
6.1.1.8. SUSE Linux Enterprise Server 11 SP2;
6.1.1.9. Novell Open Enterprise Server 11;
6.1.1.10. openSUSE Linux 12.1;
6.1.1.11. openSUSE Linux 12.2;
6.1.1.12. Mandriva Enterprise Server 5.2;
6.1.1.13. Ubuntu Server 10.04.2 LTS;
6.1.1.14. Ubuntu Server 12.04 LTS;
6.1.1.15. Debian GNU/Linux 6.0.5;
6.1.1.16. FreeBSD 8.3;
6.1.1.17. FreeBSD 9.
6.1.2. Plataforma 64-bits:

6.1.2.1. Canaima 3
6.1.2.2. Asianux Server 3 SP4
6.1.2.3. Asianux Server 4 SP1
6.1.2.4. Red Hat Enterprise Linux 6.2 Server;
6.1.2.5. Red Hat Enterprise Linux 5.8 Server
6.1.2.6. Fedora 16;
6.1.2.7. CentOS-6.2;
6.1.2.8. SUSE Linux Enterprise Server 11 SP2;
6.1.2.9. Novell Open Enterprise Server 11;
6.1.2.10. openSUSE Linux 12.1;
6.1.2.11. openSUSE Linux 12.2;
6.1.2.12. Mandriva Enterprise Server 5.2;
6.1.2.13. Ubuntu Server 10.04.2 LTS;
6.1.2.14. Ubuntu Server 12.04 LTS;
6.1.2.15. Debian GNU/Linux 6.0.5;
6.1.2.16. FreeBSD 8.3;
6.1.2.17. FreeBSD 9.

6.2. Características:

6.2.1. Deve prover as seguintes proteções:

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

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

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

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

6.2.2.2. 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;

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

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

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

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

6.2.5. 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;

6.2.6. Capacidade de verificar objetos usando heurística;

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

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

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

7. Servidores Novell Netware:

7.1. Compatibilidade:

7.1.1. Novell Netware 5.x Support Pack 6 ou superior
7.1.2. Novell Netware 6.0 Support Pack 3 ou superior
7.1.3. Novell Netware 6.5 Support Pack 3 ou superior

7.2. Características:

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

7.2.2. Deve possuir verificação manual e agendada de acordo com a configuração do administrador;
7.2.3. Capacidade de realizar update de maneira automatica, via internet ou LAN; 7.2.4. Capacidade de fazer um rollback das vacinas;
7.2.5. Capacidade de mover arquivos suspeitos ou infectados para área de quarentena;
7.2.6. Capacidade de criar logs detalhados e salvar resultados das verificações agendadas;
7.2.7. Capacidade de salvar um backup de todos os objetos infectados e suspeitos tratados;
7.2.8. Capacidade de notificar o administrador de varreduras concluidas e sobre objetos maliciosos encontrados no servidor, utilizando a rede Novell ou email;

8. Smartphones e tablets-

8.1. Compatibilidade:
8.1.1. Apple iOS 4.0, 4.1, 4.2, 4.3, 5.0, 5.1 e 6.0
8.1.2. Symbian OS 9.1, 9.2, 9.3, 9.4 Series UI 60 e Symbian^3, Symbian Anna, Symbian Belle
8.1.3. Windows Mobile 5.0, 6.0, 6.1 e 6.5
8.1.4. BlackBerry 4.5, 4.6, 4.7, 5.0, 6.0, 7.0 e 7.1 8.1.5. Android OS 1.5, 1.6, 2.0, 2.1, 2.2, 2.3, 4.0 e 4.1
8.2. Características:
8.2.1. Deve prover as seguintes proteções:
8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
8.2.1.1.1. Todos os objetos transmitidos usando conexões wireless (porta de infra-vermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.
8.2.1.1.2. Arquivos abertos no smartphone
8.2.1.1.3. Programas instalados usando a interface do smartphone
8.2.1.2. Verificação dos objetos na memória interna do smartphone e nos cartões de expanção sob demanda do usuário e de acordo com um agendamento;
8.2.2. Deverá isolar em área de quarentena os arquivos infectados;
8.2.3. Deverá atualizar as bases de vacinas de modo agendado;
8.2.4. Deverá bloquear spams de SMS através de Black lists;
8.2.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;
8.2.6. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.
8.2.7. Deverá ter firewall pessoal;
8.2.8. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Devive Manager 2008 SP1
8.2.9. Possibilidade de instalação remota utilizando o Sybase Afaria 6.5
8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS
8.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos
8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso
8.2.13. Capacidade de criar conteiners de aplicativos, separando dados corporativos de dados pessoais
8.2.14. Capacidade de configurar White e black list de aplicativos

9. Gerenciamento de dispositivos móveis (MDM):

9.1. Compatibilidade:
9.1.1. Dispositivos conectados através do Microsoft Exchange ActiveSync
9.1.1.1. Apple iOS
9.1.1.2. Symbian OS
9.1.1.3. Windows Mobile e Windows Phone
9.1.1.4. Android
9.1.1.5. Palm WebOS

9.1.2. Dispositivos com suporte ao Apple Push Notification (APNs) servisse
9.1.2.1. Apple iOS 3.0 ou superior
9.2. Caracteristicas:
9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange
9.2.2. Capacidade de ajustar as configurações de :
9.2.2.1. Sincronização de e-mail
9.2.2.2. Uso de aplicativos
9.2.2.3. Senha do usuário
9.2.2.4. Criptografia de dados
9.2.2.5. Conexão de mídia removível
9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis
9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS
9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS
9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS

10. Criptografia:

10.1. Compatibilidade:
10.1.1. Microsoft Windows XP Professional SP3
10.1.2. Microsoft Windows Vista Business/Enterprise/Ultimate SP2
10.1.3. Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2
10.1.4. Microsoft Windows 7 Professional/Enterprise/Ultimate
10.1.5. Microsoft Windows 7 Professional/Enterprise/Ultimate x64
10.1.6. Microsoft Windows 8 Professional/Enterprise
10.1.7. Microsoft Windows 8 Professional/Enterprise x64
10.1.7. Microsoft Windows 8.1 Professional/Enterprise
10.1.8. Microsoft Windows 8.1 Professional/Enterprise x64
10.2. Caracteristicas:
10.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação.
1 0.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits.
10.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário.
10.2.4. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot.
10.2.5. Permitir criar vários usuários de autenticação pré-boot.
10.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento.
10.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
10.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes.
10.2.7.2. Criptografar todos os arquivos individualmente.
10.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível
listar os arquivos e pastas armazenadas.
10.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha.
10.2.8. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários.
10.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados.
10.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados.

11. Gerenciamento de Sistemas:

11.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal.
11.2. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis.
11.3. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários.
11.4. Possuir tecnologia de Controle de Admissão de Rede (NAC), com a possibilidade de criar regras de quais tipos de dispositivos podem ter acessos a recursos da rede.
11.5. Capacidade de gerenciar licenças de softwares de terceiros.
11.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas.
11.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros.

ANEXO III – MINUTA DE CONTRATO

CONTRATO DE FORNECIMENTO DE **AQUISIÇÃO DE 300 (TREZENTAS) LICENÇAS DE SOFTWARE ANTIVÍRUS CORPORATIVO**, COM ATUALIZAÇÕES POR 24 MESES, CELEBRADO ENTRE O UNI-FACEF – CENTRO UNIVERSITÁRIO DE FRANCA, E A EMPRESA _____.

Processo nº __/2014

O **Uni-FACEF – CENTRO UNIVERSITÁRIO DE FRANCA,** situado na Av. Major Nicácio, 2433 – Bairro São José na cidade de Franca, no Estado de São Paulo, inscrito no CNPJ sob o número 47.987.136/0001-09, neste ato representado por seu Reitor, o **Sr. Alfredo José Machado Neto**, brasileiro, casado, portador da Cédula de Identidade nº 4.885.208 emitida pela SSP/SP e CPF nº 369.208.608-30 a seguir denominado simplesmente CONTRATANTE, e, de outro lado, a **Empresa _____,** inscrita no CNPJ sob o número_____/____-__, estabelecida na _____, n.º _____, Bairro _____, CEP _____-_____, cidade de _____, neste ato representada por **_____,** nacionalidade_____, estado civil_____, portador da Carteira de Identidade RG nº _____, emitida pela _____, CPF nº _____, residente e domiciliado na cidade de _____, na Rua _____, nº _____, doravante denominada simplesmente CONTRATADA, têm entre si justo e avençado e celebram por força do presente instrumento, em conformidade com o disposto na **Lei nº 10.520/2002, Decreto nº 5.450/2005, Decreto do Município de Franca nº 8.511/05 de 22/06/2005, Lei Complementar nº 123/2006**, e na **Lei Federal nº 8.666/1993** e suas alterações, **contrato de fornecimento de 300 licenças de software antivírus corporativo com assistência técnica em garantia e atualizações por 24 meses**, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - DO OBJETO - O presente contrato tem como objeto a aquisição de **_____ unidades de _____ da marca** _____, todos com as configurações constantes do presente edital e da proposta da CONTRATADA, instalados, dentro das condições previstas na proposta apresentada ao Pregão Eletrônico em epígrafe.

Parágrafo Primeiro – Os software deverão ser fornecidos com todos os itens, acessórios de necessários à sua perfeita instalação e funcionamento.

Parágrafo Segundo - Os software's deverão estar acompanhados das respectivas Notas Fiscais Eletrônicas e de sua documentação técnica completa e atualizada.

CLÁUSULA SEGUNDA - DO PREÇO - O valor total a ser pago à CONTRATADA pelos software's fornecidos por meio deste contrato é **R$ _____ (_____).**

CLÁUSULA TERCEIRA – DA GARANTIA – Os software's fornecidos serão garantidos e atualizados pelo prazo mínimo de 24 meses, conforme anexo I do Edital e nos termos da proposta apresentada.

Parágrafo Único - O CONTRATANTE poderá admitir que a Assistência Técnica seja prestada por empresa(s) da Rede Credenciada do fabricante, nas mesmas condições da CONTRATADA e sem custo adicional, desde que a operação seja previamente comunicada ao CONTRATANTE, observado o disposto no Parágrafo Único da CLÁUSULA SEXTA.

CLÁUSULA QUARTA - DA ENTREGA E DO RECEBIMENTO DOS SOFTWARE'S – Os software's deverão ser entregues na **Unidade I do Uni-FACEF**, localizada na Av. Major Nicácio, 2433 – Bairro São José, Franca-SP, CEP 14.401-135, ou disponibilizados na rede mundial de computadores, em local de acesso permitido ao Contratante.

Parágrafo Primeiro – A Reitoria do CONTRATANTE designará um responsável para recebimento dos software's fornecidos por meio deste contrato.

Parágrafo Segundo - Os softwares serão recebidos:

I - **provisoriamente**, no ato de sua entrega, por servidor designado pelo CONTRATANTE, mediante recibo aposto na respectiva nota fiscal;
II - **definitivamente**, no prazo de **cinco dias** contados do recebimento provisório, pelo responsável designado, mediante termo de recebimento.

CLÁUSULA QUINTA - DOS PAGAMENTOS - Os pagamentos serão efetuados mediante depósitos bancários, no prazo máximo de 10 (dez) dias contados a partir do recebimento definitivo do objeto licitado, mediante apresentação da nota fiscal/fatura devidamente atestada pelo setor requisitante, desde que não haja fato impeditivo provocado pela própria CONTRATADA.

Parágrafo Primeiro - É condição indispensável para que os pagamentos sejam efetuados no prazo estipulado que os documentos apresentados na fase de habilitação não se encontrem com o prazo de validade vencido, especialmente os referentes à regularidade fiscal.

Parágrafo Segundo - Enquanto não liquidada obrigação financeira imposta à CONTRATADA, em virtude de penalidade por inadimplência, os pagamentos serão efetuados com observância ao estabelecido nos Parágrafos Primeiro e Segundo da CLÁUSULA SÉTIMA deste contrato, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária.

Parágrafo Terceiro – Para todos os efeitos, considerar-se-á como data do pagamento a data de emissão da ordem bancária pelo CONTRATANTE.

CLÁUSULA SEXTA - DAS RESPONSABILIDADES DAS PARTES - São obrigações das partes, além de outras previstas em lei e neste contrato:

I - OBRIGAÇÕES DA CONTRATADA:
A CONTRATADA tem por responsabilidade, afora outras que lhe couberem por lei e por este:

a) fornecer o objeto da contração na forma e prazos estabelecidos neste contrato e no edital da licitação;
b) responder por quaisquer prejuízos, mediante a devida comprovação a ser apurada por representantes das partes, e indenizar o CONTRATANTE ou terceiros por todo e qualquer dano pessoal ou material que possa advir, direta ou indiretamente do cumprimento das obrigações decorrentes do contrato. A indenização devida será procedida pela CONTRATADA em favor do CONTRATANTE ou partes prejudicadas, independentemente de qualquer ação judicial;
c) executar os serviços com esmero e correção, refazendo tudo quanto for impugnado pela fiscalização, quer em razão do material, quer da mão-de-obra;
d) reparar ou substituir, às suas expensas, no todo ou em parte, o objeto do contrato em que forem verificados vícios, defeitos ou incorreções;
e) não transferir a outrem, no todo ou em parte, o presente contrato, sem prévia e expressa anuência do CONTRATANTE;

II - DAS OBRIGAÇÕES DO CONTRATANTE:
a) proporcionar condições indispensáveis para que a CONTRATADA possa fornecer os produtos e prestar os serviços previstos neste contrato;
b) designar servidores para o recebimento do objeto e acompanhamento do contrato;
c) proceder pontualmente ao pagamento devido à CONTRATADA.
Parágrafo Único – As obrigações contratuais são de responsabilidade exclusiva da CONTRATADA. O CONTRATANTE não aceitará, sob nenhum pretexto, a transferência dessa responsabilidade para outras pessoas físicas ou jurídicas, sejam fabricantes, técnicos ou quaisquer outros, **ainda que admitida a terceirização da assistência técnica**.

CLÁUSULA SÉTIMA - DAS PENALIDADES - O licitante que deixar de entregar quaisquer documentos exigidos no Edital ou apresentar documentação falsa para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta ou lance, não celebrar o contrato ou instrumento equivalente, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e contratar com a Administração Pública, pelo prazo de até 05 (cinco) anos, garantida a prévia defesa, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais.

I- O licitante sujeitar-se-á, ainda, às sanções de: advertência, multa e declaração de inidoneidade, sendo que as sanções de suspensão descritas no item anterior e declaração de inidoneidade poderão ser cumuladas com multa, sem prejuízo da rescisão contratual.

II- As multas poderão ser cumulativas, reiteradas e aplicadas em dobro, sempre que se repetir o motivo.

III- Ocorrendo atraso na execução/entrega do objeto contratado será aplicada multa moratória de **0,3%** (zero vírgula três por cento) por dia de atraso, até o limite de **20 %** (vinte por cento) sobre o valor total do contrato.

IV- No descumprimento de quaisquer obrigações licitatórias/contratuais, poderá ser aplicada multa indenizatória de **10%** (dez por cento) do valor total do objeto licitado.

V- A multa, aplicada após regular processo administrativo, será descontada da(s) fatura(s), cobrada judicialmente ou extrajudicialmente, a critério do contratante.

VI- Da intenção de aplicação de quaisquer das penalidades previstas, será concedido prazo para defesa prévia de 5 (cinco) dias úteis a contar da notificação.

VII- Da aplicação da sanção caberá recurso no prazo de 05 (cinco) dias úteis a contar da sua publicação.

VIII- As penalidades serão obrigatoriamente registradas, esgotada a fase recursal, no Cadastro de Fornecedores do Município, no caso de impedimento do direito de licitar e contratar, o licitante terá seu cadastro cancelado por igual período.

CLÁUSULA OITAVA - DOS RECURSOS - Dos atos da Administração cabe recurso, obedecido o disposto no art. 109 da Lei nº 8.666/93.

Parágrafo único - O recurso interposto deverá ser protocolizado na Secretaria do Uni-FACEF, localizada na Av. Major Nicácio, 2433 – Bairro São José, Franca-SP, de Segunda a Sexta-feira, das 07:30 às 16:30 horas.

CLÁUSULA NONA - NATUREZA DA DESPESA - Os recursos financeiros serão atendidos por verbas próprias, constantes do orçamento vigente, a saber:

- 03.01.01 – Centro Universitário de Franca
- 3.3.90.39 – Outros Serviços de Terceiros – Pessoa Jurídica
- 3.3.90.39.11.001 – Locação de Softwares
- Ficha 12

CLÁUSULA DÉCIMA - VIGÊNCIA - O presente contrato vigorará desde sua assinatura até o término do prazo de garantia oferecido pela CONTRATADA, que é de 02 (dois) anos, nos termos da proposta apresentada após o recebimento definitivo dos software.

CLÁUSULA ONZE – DA DOCUMENTAÇÃO COMPLEMENTAR - Fazem parte integrante do presente contrato, independentemente de transcrição, o Edital de Pregão Eletrônico e seus anexos, a Proposta de Preços da CONTRATADA e sua documentação de habilitação, constantes do Processo.

CLÁUSULA DOZE – DA RESCISÃO - São motivos para a rescisão do contrato os relacionados no artigo 78 da Lei 8.666/93.

Parágrafo Primeiro - A inexecução total ou parcial deste contrato enseja a sua rescisão, com as conseqüências contratuais e as previstas em lei.
Parágrafo Segundo - A rescisão do contrato atenderá ao disposto no art. 79 da Lei 8.666/93.

CLÁUSULA TREZE – DO FORO - Fica eleito o Foro de Franca estado de São Paulo, para dirimir quaisquer dúvidas ou contestações oriundas direta ou indiretamente deste Contrato, que não possam ser resolvidas por meios administrativos, renunciando-se expressamente a qualquer outro, por mais privilegiado que seja.

E para firmeza e como prova de assim haverem entre si ajustado e contratado, é lavrado o presente contrato, que, depois de lido e achado conforme, é assinado pelas partes contratantes, em 3 (três) vias de igual teor e de mesmos efeitos legais.

Franca (SP), ___ de _____ de 2014.

Prof. Dr. Alfredo José Machado Neto	Representante legal
Reitor do Uni-FACEF	Empresa

Testemunhas:

Nome	Nome
CPF	CPF

ANEXO IV – MODELO: DECLARAÇÃO - ART. 7º CF

DECLARAÇÃO DE OBSERVÂNCIA AO DISPOSTO NO INCISO XXXIII DO ART. 7º DA CONSTITUIÇÃO FEDERAL

Deve ser impressa em papel timbrado da empresa participante na licitação

PROCESSO Nº 13/2014
PREGÃO ELETRÔNICO Nº 07/2014

Objeto: **AQUISIÇÃO DE 300 (TREZENTAS) LICENÇAS DE SOFTWARE ANTIVÍRUS CORPORATIVO.**

PROPONENTE: _____

CNPJ: _____

ENDEREÇO: _____

Declaramos, para os fins de direito que esta empresa cumpre integralmente a norma contida na Constituição da República Federativa do Brasil de 1988, do art. 7º, inciso XXXIII, a saber:

> *"(...) proibição de trabalho noturno, perigoso ou insalubre a menores de dezoito anos e qualquer trabalho a menores de dezesseis anos, salvo na condição de aprendiz a partir de quatorze anos*".

Esta declaração é parte integrante da documentação exigida pelo Edital da licitação, modalidade Pregão Nº **07/2014**, do Centro Universitário de Franca, e por ela responde integralmente a declarante.

Por ser a expressão da verdade, firmamos a presente.

.....(local e data)

.....
Nome completo do Declarante
RG / CPF
Cargo
Carimbo CNPJ

ANEXO V – MODELO: DECLARAÇÃO ME/EPP

DECLARAÇÃO DE ENQUADRAMENTO ME/EPP
Deve ser impressa em papel timbrado da empresa participante na licitação

PROCESSO Nº 13/2014
PREGÃO ELETRÔNICO Nº 07/2014

Objeto: **AQUISIÇÃO DE 300 (TREZENTAS) LICENÇAS DE SOFTWARE ANTIVÍRUS CORPORATIVO.**

PROPONENTE: _____

CNPJ: _____

ENDEREÇO: _____

Declaramos para os devidos fins que a empresa (Nome da empresa), CNPJ (número CNPJ) estabelecida na (rua; nº e cidade), por seu representante legal (nome do representante, RG), declara, sob as penas da lei penal e civil, que a ora declarante está classificada na presente data como Microempresa – ME / Empresa de Pequeno Porte – EPP perante a (Receita Federal e/ou Secretaria da Fazenda do Estado), comprometendo-se ainda a informar caso deixe de ser enquadrada em tal condição, nos termos da lei.

.....(local e data)

.....
Nome completo do Declarante
RG / CPF
Cargo
Carimbo CNPJ

ANEXO VI – MODELO: DECLAR. INEXIST. DE FATO IMPEDITIVO

DECLARAÇÃO DE INEXISTÊNCIA DE FATO SUPERVENIENTE IMPEDITIVO

Deve ser impressa em papel timbrado da empresa participante na licitação

PROCESSO Nº 13/2014
PREGÃO ELETRÔNICO Nº 07/2014

Objeto: **AQUISIÇÃO DE 300 (TREZENTAS) LICENÇAS DE SOFTWARE ANTIVÍRUS CORPORATIVO.**

A Empresa (nome da empresa), sediada na Rua (endereço completo da empresa), inscrita no Cadastro Nacional de Pessoa Jurídica (CNPJ) sob o nº (número CNPJ), por seu representante legal (nome do representante), CPF (número do documento), DECLARA, sob as penas da lei, a INEXISTENCIA de fatos supervenientes, que impossibilitem sua participação no Pregão nº **07/2013**, pois que encontram-se satisfeitas as exigências previstas no art. 27 da Lei 8.666/93, e suas alterações.

.....(local e data)

.....
Nome completo do Declarante
RG / CPF
Cargo
Carimbo CNPJ

ANEXO VII – MODELO: PROPOSTA DE PREÇOS

PROPOSTA DE PREÇOS

Deve ser impressa em papel timbrado da empresa participante na licitação

PROCESSO Nº 13/2014
PREGÃO ELETRÔNICO Nº 07/2014

Objeto: **AQUISIÇÃO DE 300 (TREZENTAS) LICENÇAS DE SOFTWARE ANTIVÍRUS CORPORATIVO.**

PROPONENTE:
CNPJ:
ENDEREÇO:
TELEFONE/FAX:
E-MAIL DE CONTATO:

Validade da proposta: 60 (sessenta) dias corridos, a contar da data de abertura dos envelopes.

PLANILHA DE PREÇOS:

LOTE	DESCRIÇÃO	VALOR UNITÁRIO	QUANT.	VALOR TOTAL
01		**R$**	**300**	**R$**

Declaração: Declaro-me expressamente de acordo com as normas e condições constantes do Edital do Pregão Eletrônico nº **07/2014**, submetendo-me aos termos que o integram.

.....(local e data)

.....
Nome completo do Representante
RG / CPF
Cargo
Carimbo CNPJ