TERMO DE CONTRATO 58/2016

CONTRATO DE **FORNECIMENTO DE LICENÇA DE SOFTWARE ANTIVÍRUS CORPORATIVO**, COM ATUALIZAÇÕES POR 24 MESES, CELEBRADO ENTRE O CENTRO UNIVERSITÁRIO MUNICIPAL DE FRANCA – UNI-FACEF, E A EMPRESA **FORT SECURE TECNOLOGIA LTDA ME**.

Processo nº 27/2016

OBJETO: FORNECIMENTO DE LICENÇA DE SOFTWARE ANTIVÍRUS CORPORATIVO	
Data assinatura: 23/09/2016	**Valor Global: R$ 53.440,00**
Vigência/Execução: de 03/10/2016 a 02/10/2018	

Razão Social:	**FORT SECURE TECNOLOGIA LTDA ME**				
Endereço:	Rua José Bianchi, nº 555 sala 1716. Bairro: Nova Ribeirânia. Ribeirão Preto/ SP				
CEP:	14.096-730	**CNPJ**	**12.641.727/0001-37**	**TEL:**	(16) 3877-8033
Representante	Danilo Penna Vicentine		**CPF:**	262.816.908-85	
e-mail:	danilo@fortsecure.com.br		**RG:**	24.309.996-4	

O CENTRO UNIVERSITÁRIO MUNICIPAL DE FRANCA – Uni-FACEF**,** 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, professor, portador do RG n.º 4.885.208, inscrito no CPF/MF sob o nº 369.208.608-30, a seguir denominado simplesmente CONTRATANTE, e, de outro lado, a Empresa e seu representante devidamente identificados no quadro presente no caput deste termo contratual **FORT SECURE TECNOLOGIA LTDA ME**, daqui por diante 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**, **nº 10.520, de 17 de julho de 2002**, e na **Lei Federal nº 8.666/1993** e suas alterações, **contrato de fornecimento de 320 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 **320 unidades de licença de software antivírus corporativo da marca Kaspersky**, 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.

LOTE	QTDE	DESCRIÇÃO	MARCA	VLR UNITÁRIO	VLR TOTAL
1	320	Kaspersky Endpoint Security for Business- Advanced Brazilian Edition, 250-499 node 2 year	Kaspersky	R$ 167,00	R$53.440,00

Parágrafo Primeiro – Os software's 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$ 53.440,00 (cinquenta e três mil quatrocentos e quarenta reais).**

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 15 (quinze) dias contados a partir do recebimento definitivo do objeto licitado, mediante apresentação da nota fiscal eletrônica 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 Uni-FACEF, 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 07h30min às 16h30min.

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

03.01.01 – Centro Universitário Municipal de Franca
Elemento: 3.3.90.39 – Outros Serviços de Terceiros – Pessoa Jurídica

CLÁUSULA DÉCIMA - VIGÊNCIA - O presente contrato vigorará a partir de 03/10/2016 até 02/10/2018, 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's. Sendo este período prorrogável a critério da Administração nos termos do artigo 57 da Lei n° 8.666/1993.

CLAUSULA DÉCIMA PRIMEIRA – DOS ADITAMENTOS E DOS PREÇOS
11.1. Aplica-se ao presente contrato as disposições dos artigos 57 e 65 da Lei nº 8.666/93, que deverá ser formalizada por termos aditivos, caso haja interesse do Contratante.

11.2. Os preços que vigorarão no contrato durante os primeiros 24 meses contratados corresponderão aos valores propostos, com data base do mês da proposta, que poderão ser reajustados por índice negociado entre os contratantes, nunca superior à variação do IGP-M da Fundação Getúlio Vargas (FGV) ou outro índice que vier a substituí-lo, nos casos dos aditamentos previstos no item 11.1.
11.2.1. Os referidos preços constituirão, a qualquer título, a única e completa remuneração pela execução contratual e pelo pagamento de quaisquer encargos dela resultantes.

CLÁUSULA DÉCIMA SEGUNDA – 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 DÉCIMA TERCEIRA – 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 consequências contratuais e as previstas em lei.
Parágrafo Segundo - A rescisão do contrato atenderá ao disposto no art. 79 da Lei 8.666/93.

CLÁUSULA DÉCIMA QUARTA – 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), 23 de setembro de 2016.

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

Danilo Penna Vicentine
Fort Secure Tecnologia Ltda ME

Testemunhas:

Fernando Silva Tonus
CPF: 353.257.258-31

Alessandro Rodrigues da Silva
CPF: 159.821.378-61

ANEXO II - DESCRIÇÃO DO OBJETO E ESPECIFICAÇÕES

PROCESSO LICITATÓRIO: Erro! Fonte de referência não encontrada./**2016**
MODALIDADE: PREGÃO ELETRÔNICO **Nº** Erro! Fonte de referência não ncontrada./**2016**
TIPO: MENOR PREÇO **FINALIDADE: CONTRATAÇÃO**

Objeto: Erro! Fonte de referência não encontrada..

LOTE 01 – SOFTWARE ANTIVÍRUS CORPORATIVO

QUANTIDADE: 320 (trezentas e vinte)
UNIDADE: licença
DESCRIÇÃO: Software Antivírus Corporativo

Características e Especificações (Atributos Técnicos Mínimos Obrigatórios):

1 Ferramentas de proteção para servidores Windows e Linux:

1.1 Deve possuir suporte técnico especializado aos sistemas operacionais baseados nas plataformas:

1.1.1 Windows Server 2003, 2008 ou superior (qualquer edição e arquitetura, 32 ou 64 bits) e Linux nas distribuições Red Hat Enterprise 5 e CentOS 5.5 ou superiores (arquiteturas de 32 ou 64 bits).

1.2 Deve permitir instalação e atualização do programa de antivírus e das vacinas de maneira remota;

1.3 Deve permitir instalação e atualização do programa de antivírus e das vacinas com o servidor desconectado da rede, por meio de mídia removível;

1.4 Deve permitir instalação e atualização do programa de antivírus e das vacinas via script, sem requerer outro software;

1.5 Deve permitir atualização automática de vacinas, de forma incremental, e outros componentes do software;

1.6 Deve possuir formas de configuração de atualização de clientes descentralizada, ou seja, através dos próprios clientes ou outros agentes que serão responsáveis por atualizar LANs específicas, com o intuito de minimizar o tráfego de rede WAN. O horário de atualização deve ser configurável e a atualização deve permitir conexão através de serviço proxy;

1.7 Deve permitir detecção (por intermédio de assinaturas, heurística, por comportamento e reputação de arquivos), limpeza e remoção de vírus, vírus de macro, "*Trojan Horse*", Worms, ferramentas maliciosas, *spywares*, *adwares*, *cookies*, *rootkits* e outros tipos de ameaças;

1.8 Deve permitir a possibilidade de restauração do arquivo original após a remoção dos itens: vírus, vírus de macro, "*Trojan Horse*", *Worms*, ferramentas maliciosas, *spywares*, *adwares*, *cookies*, *rootkits* e outros tipos de ameaças;

1.9 Deve possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos e que não possam ser reparados no cliente;

1.10 Deve permitir um gerenciamento da quarentena, podendo isolar (tornar inacessível)

ou apagar arquivos que estiverem nela;
1.11 Deve permitir detecção e remoção, em tempo real, de artefatos maliciosos carregados em memória. Caso o arquivo infectado não possa ser limpo, deverá ser automaticamente excluído ou movido para área de segurança (quarentena) conforme configuração pré-definida;
1.12 Deve possuir proteção contra *Spywares* ou outros artefatos maliciosos, sem a necessidade de um software ou agente adicional;
1.13 Deve permitir a possibilidade de retorno à versão anterior das vacinas;
1.14 Deve permitir a instalação da ferramenta de proteção (cliente) sem necessidade de reiniciar o servidor;
1.15 Deve detectar a incidência de vírus não permitindo que eles danifiquem os arquivos e/ou diretórios;
1.16 Deve permitir a proteção contra desinstalação, desativação e alteração de configurações de forma não autorizada do cliente de proteção;
1.17 Deve permitir a realização de varredura (*scan*) manual, agendado e em tempo real nos servidores;
1.18 Deve permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim a performance do produto mais estável;
1.19 Deve permitir a varredura (*scan*) de arquivos compactados, pelo menos nos formatos ZIP, TAR, RAR, CAB, ARJ, no mínimo, em três níveis de compactação;
1.20 Deve permitir a varredura otimizada com analise de alteração de arquivos, ou seja, arquivos já escaneados e não alterados, não devem ser analisados nas próximas varreduras, mesmo após o reinicio do equipamento;
1.21 Deve possuir a capacidade de procurar códigos maliciosos pelo tipo real de arquivo;
1.22 Deve possuir programação de rastreamentos automáticos do sistema com as seguintes opções:
- 1.22.1 Escopo: Todos os drives locais, drives específicos, ou pastas específicas;
- 1.22.2 Ação: Somente alertas, limpar automaticamente, apagar automaticamente, ou mover automaticamente para área de segurança (quarenta);
- 1.22.3 Frequência: Diária, semanal, mensal;
- 1.22.4 Exclusões: Pastas, arquivos ou extensões de arquivos que não devem ser rastreados.

1.23 Deve permitir a possibilidade de varredura manual de arquivos, diretórios, dispositivos físicos ou removíveis, através de opção com o botão direito do mouse.
1.24 A ferramenta deverá possuir opção para restringir varreduras em compartilhamentos de rede por grupos de estações, usuários ou senha.
1.25 Deve possuir log centralizado contendo, no mínimo, os seguintes itens:
- 1.25.1 Nome do vírus;
- 1.25.2 Nome do arquivo infectado;
- 1.25.3 Data e hora da infecção;
- 1.25.4 Ação tomada;
- 1.25.5 Usuário logado na máquina.
- 1.25.6 Nome da máquina;
- 1.25.7 IP.

1.26 Deve possuir notificação automática via e-mail ou mensagem XMPP ou SNMP ao administrador em caso de uma ou mais máquinas serem infectadas;

1.27 Deve permitir gerar listas de exclusões dos itens: vírus, vírus de macro, "*Trojan Horse*", *Worms*, ferramentas maliciosas, *spywares*, *adwares*, *cookies*, *rootkits* e outros tipos de ameaças para que eles não sejam removidos;
1.28 Deve possuir, no mínimo, duas ações automáticas (limpeza/deleção) para tratamento de arquivos infectados com códigos maliciosos. Caso a primeira ação falhe, a segunda deverá ser executada;
1.29 Deve permitir a possibilidade de colocar arquivos, extensões de arquivos ou diretórios em listas de exclusões para não serem verificados pelo antivírus;
1.30 Após a atualização da lista de assinaturas de vírus a maquina não deve necessitar ser reiniciada;
1.31 Deve permitir atualização manual das assinaturas de vírus, caso o cliente não esteja conectado na rede;
1.32 Deve permitir configuração de política específica para atualização automática das assinaturas de vírus via internet, caso o cliente não esteja conectado na rede interna;
1.33 A solução deve manter compatibilidade com os *kernels Linux* e produtos da família Windows a serem lançados, posteriormente à assinatura do contrato;
1.34 Deve permitir a possibilidade de funcionamento independente da ferramenta de gerenciamento centralizado;
1.35 Deve possuir instalação "silenciosa";
1.36 Deve permitir a personalização de mensagens de alertas e a possibilidade de supressão de sua exibição na máquina cliente;
1.37 Deve permitir a possibilidade de geração de imagem do servidor com o antivírus instalado;
1.38 Em caso de parada na proteção, o serviço de antivírus deve ser capaz de reiniciar automaticamente após a parada;
1.39 Deve possuir a capacidade de monitorar e bloquear as invasões por proteção comportamental; 4.1.40 Deve possuir IDS/IPS integrado à solução;
1.41 A substituição de servidores antigos por novos, não implicará no pagamento de novos serviços;
1.42 Deve possuir capacidade de bloquear execução de aplicativos em diretórios ou dispositivos de armazenamento específicos, bem como a criação, via console de gerenciamento, de exceções a esta política por meio de impressão digital (mecanismo de assinatura que identifique unicamente o executável) dos executáveis autorizados de modo que somente as aplicações que possuam suas impressões digitais cadastradas, possam ser executadas;
1.43 A solução deve possuir a capacidade de bloquear dispositivos externos conectados via interface USB, tais como: dispositivos de armazenamento em massa (exemplo: Pen-drivers), smartphones; bem como criar regras de exceção a esta política.

2 Ferramenta de proteção de estações de trabalho (desktops e notebooks):

2.1 Deve possuir suporte técnico especializado aos sistemas operacionais baseados nas plataformas:
2.1.1 Windows XP, 7, 8, 8.1, 10 e superiores (qualquer edição e arquitetura, 32 ou 64 bits);
2.2 Deve permitir instalação e atualização do programa de antivírus e das vacinas de

maneira remota;
2.3 Deve permitir instalação e atualização do programa de antivírus e das vacinas com a estação desconectada da rede, por meio de mídia removível;
2.4 Deve permitir instalação e atualização do programa de antivírus e das vacinas via script, sem requerer outro software;
2.5 Deve permitir a atualização automática das vacinas, de forma incremental, e dos componentes do software;
2.6 Deve possuir formas de configuração de atualização de clientes descentralizada, ou seja, através dos próprios clientes ou outros agentes que serão responsáveis por atualizar LANs especificas, com o intuito de minimizar o trafego de rede WAN. O horário de atualização deve ser configurável e a atualização deve permitir conexão através de serviço proxy;
2.7 Deve permitir a detecção (por intermédio de assinaturas, heurística, por comportamento e reputação de arquivos), limpeza e remoção de vírus, vírus de macro, "*Trojan Horse", Worms*, ferramentas maliciosas, *spywares*, *adwares*, *cookies*, *rootkits* e outros tipos de ameaças;
2.8 Deve permitir a possibilidade de restauração do arquivo original após a remoção dos itens: vírus, vírus de macro, "*Trojan Horse*", *Worms*, ferramentas maliciosas, spywares, adwares, cookies, rootkits e outros tipos de ameaças;
2.9 Deve possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos e que não possam ser reparados no cliente;
2.10 Deve permitir um gerenciamento da quarentena, podendo isolar (tornar inacessível) ou apagar arquivos que estiverem nela;
2.11 Deve possuir detecção e remoção, em tempo real, de artefatos maliciosos carregados em memória. Caso o arquivo infectado não possa ser limpo, deverá ser automaticamente excluído ou movido para área de segurança (quarentena) conforme configuração pré-definida;
2.12 Deve possuir proteção contra *Spywares* ou outros artefatos maliciosos, sem a necessidade de um software ou agente adicional;
2.13 Deve permitir a possibilidade de retorno à versão anterior das vacinas;
2.14 Deve permitir a instalação da ferramenta de proteção (cliente) sem necessidade de reiniciar a estação de trabalho;
2.15 A solução de antivírus deve detectar a incidência de vírus não permitindo que eles danifiquem os arquivos e/ou diretórios;
2.16 Deve permitir a proteção contra desinstalação, desativação e alteração de configurações de forma não autorizada do cliente de proteção;
2.17 Deve permitir a realização de varredura (scan) manual, agendado e em tempo real nas estações;
2.18 Deve permitir diferentes configurações de desempenho de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim a performance do produto mais estável;
2.19 Deve possuir varredura (*scan*) de arquivos compactados, pelo menos nos formatos ZIP, TAR, RAR, CAB, ARJ, no mínimo, em três níveis de compactação;
2.20 Deve possuir varredura otimizada com analise de alteração de arquivos, ou seja, arquivos já escaneados e não alterados, não devem ser analisados nas próximas

varreduras, mesmo após o reinicio do equipamento;
2.21 Deve possuir capacidade de procurar códigos maliciosos pelo tipo real de arquivo;
2.22 Deve permitir a programação de rastreamentos automáticos do sistema com as seguintes opções:
2.22.1 Escopo: Todos os drives locais, drives específicos, ou pastas específicas;
2.22.2 Ação: Somente alertas, limpar automaticamente, apagar automaticamente, ou mover automaticamente para área de segurança (quarenta);
2.22.3 Frequência: Diária, semanal, mensal;
2.22.4 Exclusões: Pastas, arquivos ou extensões de arquivos que não devem ser rastreados.
2.23 Deve permitir a possibilidade de varredura manual de arquivos, diretórios, dispositivos físicos ou removíveis, através de opção com o botão direito do mouse;
2.24 A ferramenta deverá possuir opção para restringir varreduras em compartilhamentos de rede por grupos de estações, usuários ou senha;
2.25 Deve possuir log centralizado contendo no mínimo os seguintes itens:
2.25.1 Nome do vírus;
2.25.2 Nome do arquivo infectado;
2.25.3 Data e hora da infecção;
2.25.4 Ação tomada;
2.25.5 Usuário logado na máquina.
2.25.6 Nome da máquina;
2.25.7 IP.
2.26 Deve possuir notificação automática via e-mail ou mensagem XMPP ou SNMP ao administrador em caso de uma ou mais máquinas sejam infectadas;
2.27 Deve permitir gerar listas de exclusões dos itens: vírus, vírus de macro, "*Trojan Horse*", *Worms*, ferramentas maliciosas, *spywares*, *adwares*, *cookies*, *rootkits* e outros tipos de ameaças para que os mesmos não sejam removidos;
2.28 Deve possuir, no mínimo, duas ações automáticas (limpeza/deleção) para tratamento de arquivos infectados com códigos maliciosos. Caso a primeira ação falhe, a segunda deverá ser executada;
2.29 Deve permitir a possibilidade de colocar arquivos, extensões de arquivos ou diretórios em listas de exclusões para não serem verificados pelo antivírus;
2.30 Após a atualização da lista de assinaturas de vírus a máquina não deve necessitar ser reiniciada;
2.31 Deve permitir atualização manual das assinaturas de vírus, caso a estação não esteja conectada na rede;
2.32 Deve permitir a configuração de política específica para atualização automática das assinaturas de vírus via internet, caso o cliente não esteja conectado na rede interna;
2.33 A solução deve manter compatibilidade com os produtos da família Windows a ser lançados, posteriormente a assinatura do contrato;
2.34 Possibilidade de funcionamento independente da ferramenta de gerenciamento centralizado;
2.35 Possuir instalação "silenciosa";
2.36 Permitir a personalização de mensagens de alertas e a possibilidade de supressão de sua exibição na máquina cliente;
2.37 Possibilidade de geração de imagem de estação de trabalho com o antivírus

instalado;
2.38 Em caso de parada na proteção, o serviço de antivírus deve ser capaz de reiniciar automaticamente após a parada;
2.39 Deve possuir a capacidade de monitorar e bloquear as invasões por proteção comportamental;
2.40 Deve possuir IDS/IPS integrado;
2.41 Deve possuir capacidade de bloquear execução de aplicativos em diretórios ou dispositivos de armazenamento específicos, bem como a criação, via console de gerenciamento, de exceções a esta política por meio de impressão digital (mecanismo de assinatura que identifique unicamente o executável) dos executáveis autorizados de modo que somente as aplicações que possuam suas impressões digitais cadastradas, possam ser executadas;
2.42 A solução deve possuir a capacidade de bloquear dispositivos externos conectados via interface USB, tais como: dispositivos de armazenamento em massa (exemplo: Pen-drivers), smartphones; bem como criar regras de exceção a esta política.

3 Módulo para Gerenciamento da solução Antivírus – Gerência centralizada de estações e servidores:

3.1 Deve ser do mesmo fabricante das ferramentas de proteção;
3.2 Deve possuir suporte a instalação do servidor nas plataformas Windows Server 2003, 2008 ou superior;
3.3 Deve permitir o gerenciamento centralizado via web browsers ou console instalada em servidor e em estações de trabalho;
3.4 Deve permitir a criação de perfis de usuários com diferentes níveis de acesso ao console de gerenciamento;
3.5 Deve permitir a possibilidade de agrupamento das estações de trabalho e servidores, com configuração de políticas específicas para cada grupo;
3.6 Deve permitir armazenar todos os logs provenientes das ferramentas de proteção às estações de trabalho e aos servidores;
3.7 Deve gerar, no mínimo, os relatórios abaixo descritos de maneira gráfica, escolhendo o período de consulta desejado e permitindo sua exportação para os seguintes formatos: CSV, HTML, XLS, DOC, RTF, PDF ou TXT:
3.7.1 Listagem dos vírus e outros tipos de ameaças que infectaram determinada estação;
3.7.2 Listagem das estações que estão infectadas por determinado vírus;
3.7.3 Relatório dos totais de itens: vírus, vírus de macro, “Trojan Horse”, Worms, ferramentas maliciosas, spywares, adwares, cookies, rootkits e outros tipos de ameaças;
3.7.4 Listagem das estações nas quais o antivírus deixou de remover algum vírus;
3.7.5 Número total de arquivos maliciosos removidos por tipo de arquivo;
3.7.6 Relatório dos malwares (vírus, vírus de macro, “Trojan Horse”, Worms, ferramentas maliciosas, spywares, adwares, cookies, rootkits e outros tipos de ameaças) mais detectados;
3.7.7 Relatório de máquinas com maior número de infecções;
3.7.8 Relatório da eficácia de remoção dos itens descritos em XX.3.7;

3.7.9 Relatório de atualização de componentes do software antivírus e assinaturas;
3.7.10 Relatório das máquinas que não se comunicaram com o servidor antivírus a partir de uma determinada data.
3.8 Deve emitir relatórios detalhados, em formato CSV, HTML, XLS, DOC, RTF, PDF ou TXT, sobre o status de toda a solução;
3.9 Deve emitir relatórios de gerência personalizáveis;
3.10 Deve permitir a possibilidade de, no mínimo, iniciar a varredura (scan) e a atualização de definições de vírus de um ou mais clientes, a partir da console de gerência remota;
3.11 Deve descobrir, automaticamente, as estações da rede que não possuem o cliente instalado com opção de instalação remota;
3.12 Deve permitir a possibilidade de bloqueio do acesso às configurações das estações de trabalho e servidores a partir da console de gerência;
3.13 Deve possuir notificação automática via e-mail ou mensagem XMPP ou SNMP ao administrador em caso de uma ou mais máquinas serem infectadas;
3.14 Deve atualizar e implementar políticas de segurança para toda a solução em caso de epidemia, restaurando as configurações originais ao fim dessa;
3.15 Deve permitir criar planos de distribuição das atualizações;
3.16 Deve possuir serviço de verificação remoto, manual e agendado, que detecte, limpe ou remova danos causados pelos itens: vírus, vírus de macro, "Trojan Horse", Worms, ferramentas maliciosas, spywares, adwares, cookies, rootkits e outros tipos de ameaças;
3.17 Deve fornecer, em tempo real, o estado atualizado das estações de trabalho e dos servidores, com no mínimo as seguintes informações: data das vacinas, versão do antivírus, status da máquina (online ou offline), nome da máquina, usuário e IP;
3.18 Deve distribuir pacotes de correções (*patches*) do antivírus automaticamente para as estações de trabalho e servidores gerenciados;
3.19 Capacidade de gerenciar um inventário de hardware com a possibilidade de cadastro de dispositivos como, por exemplo: roteadores, switches, projetores, acessório e outros informando data de compra local onde se encontra service tag número de identificação o e outros.
3.20 Capacidade de registrar mudanças de hard are nas máquinas gerenciadas.
3.21 Deve possuir capacidade de configurar políticas de uso de dispositivos, por meio de controles de acesso e também sobre o tipo de dispositivo permitido.
3.22 Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução o e para computadores bare-metal.
3.23 Capacidade de detectar softwares de terceiros vulneráveis criando assim um relatório de softwares vulneráveis.
3.24 Capacidade de corrigir as vulnerabilidades de softwares a sendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários.
3.25 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.
3.26 Capacidade de gerenciar licenças de softwares de terceiros.