EDITAL DE LICITAÇÃO – PREGÃO ELETRÔNICO CRCRS 15/2016

PROCESSO ADMINISTRATIVO 104/2016

SOLUÇÃO ANTIVÍRUS

CONSELHO REGIONAL DE CONTABILIDADE DO RIO GRANDE DO SUL, entidade de fiscalização do exercício profissional contábil, criado pelo Decreto-Lei nº 9.295/46, com sede na Avenida Praia de Belas nº 1.554, Porto Alegre, RS, torna público a todos os interessados, realização do Pregão Eletrônico em epígrafe, para execução do objeto abaixo descrito, que se regerá pela Lei nº 8.666/93, pela Lei nº 10.520/02, Lei Complementar nº 123/06, Decreto nº 8.538/15, Decreto nº 5.450/05, bem como pelas condições estabelecidas neste Edital.

1. DO OBJETO

O objeto da presente Licitação é a aquisição de licenças de Software Antivírus com fornecimento de 180 licenças para estações de trabalho, dispositivos móveis e servidores, incluindo instalação, configuração e serviço de suporte “ON SITE” durante os primeiros 180 dias, contados da implementação, contemplando atualizações do banco de dados de ameaças, por um período de 3 anos, conforme especificações do Anexo I ao presente Edital.

2. CRITÉRIO DE ACEITAÇÃO DO OBJETO

O objeto será adjudicado ao licitante que ofertar o **menor valor global**.

3. DO LOCAL DO PREGÃO, DATA, HORÁRIO E INFORMAÇÕES

3.1. LOCAL DA DISPUTA: **www.pregaoonlinebanrisul.com.br**

3.2. DATA: **27/12/2016.**

3.3. RECEBIMENTO DAS PROPOSTAS: das 09h00min do dia 15/12/2016 até as 09h00min, do dia 27/12/2016.

3.4. ABERTURA DAS PROPOSTAS: às 09h01min, do dia 27/12/2016;

3.5. INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: **09h30min** do dia **27/12/2016.**

3.6. Ocorrendo a decretação de feriado ou qualquer fato superveniente que impeça a realização do certame na data marcada, todas as datas constantes deste Edital serão

transferidas, automaticamente, para o primeiro dia útil, ou de expediente normal, subsequente ao ora fixado;

3.7. Na contagem de todos os prazos estabelecidos neste Edital, excluir-se-á o dia de início e incluir-se-á o do vencimento, e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário;

3.8. Para todas as referências de tempo será observado o horário de Brasília (DF);

3.9. Em nenhuma hipótese serão recebidas propostas fora do prazo estabelecido neste Edital.

4. DOS PEDIDOS DE ESCLARECIMENTO

4.1. Os esclarecimentos quanto ao Edital e seus Anexos poderão ser solicitados por qualquer pessoa até 3 (três) dias úteis antes da data fixada para recebimento das propostas.

4.2. Os esclarecimentos deverão ser feitos exclusivamente por meio de correspondência eletrônica dirigida ao pregoeiro no endereço **caue@crcrs.org.br**.

4.3. Os esclarecimentos encontrar-se-ão à disposição no site www.pregaoonlinebanrisul.com.br.

5. DA IMPUGNAÇÃO

5.1 – Até dois dias úteis antes da data limite para recebimento das propostas, qualquer pessoa poderá impugnar o ato convocatório.

5.2 – Caberá ao Pregoeiro decidir sobre a petição no prazo de vinte e quatro horas.

5.3 – Acolhida a petição contra o ato convocatório, será designada nova data para a realização do certame, caso a alteração no edital influencie na formulação das propostas.

5.4 - As impugnações deverão ser protocoladas na sede do CRCRS, à Avenida Praia de Belas 1.554, Porto Alegre-RS, CEP 90.110-000.

6. DA PARTICIPAÇÃO

6.1 – Nos termos do art. 48, I da Lei Complementar 123/06, poderão participar deste pregão **exclusivamente microempresas** ou **empresas de pequeno porte.**

6.2 – Não poderão participar da presente licitação pessoas jurídicas:

a) declaradas inidôneas por órgão ou entidade da Administração Pública direta ou indireta, federal, estadual, municipal ou do Distrito Federal;

b) que se encontrem sob falência, concordata, recuperação judicial, concurso de credores, dissolução e liquidação;

c) nas quais conselheiros, delegados, empregados do Sistema CFC/CRCs e seus cônjuges ou parentes até terceiro grau atuem como sócios, proprietários, prepostos, empregados ou mediante qualquer outro vínculo jurídico;

6.3 – A participação na presente licitação implica para a Licitante a aceitação plena e irrevogável de todos os termos, cláusulas e condições constantes neste Edital e de seus anexos, a observância dos preceitos legais e regulamentares em vigor e a responsabilidade pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase do processo.

6.4. A participação dos interessados, no dia e hora fixados, dar-se-á por meio da digitação da senha privativa da licitante e subsequente encaminhamento da proposta de preços com valores unitários e totais, exclusivamente por meio eletrônico.

6.5. A informação de dados para acesso deve ser feita na página inicial www.pregaoonlinebanrisul.com.br.

7. CREDENCIAMENTO

7.1. No presente feito licitatório somente poderá se manifestar, em nome da Licitante, a pessoa por ela credenciada.

7.2. O credenciamento dos licitantes dar-se-á pelas atribuições de chave de identificação e de senha pessoal e intransferível para acesso ao sistema obtidos junto à Seção de Cadastro da Central de Licitações do Estado – CELIC.

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

7.4. O credenciamento e sua manutenção no respectivo cadastro dependerá de registro cadastral na CELIC.

7.5. O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo à PROCERGS ou ao CRCRS responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

7.6. A perda da senha ou quebra do sigilo deverão ser comunicados imediatamente à Seção de Cadastro CELIC, para imediato bloqueio de acesso.

8. DA PROPOSTA DE PREÇOS

8.1 – A licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras sua proposta e lances.

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

8.3 – O encaminhamento da proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação e das especificações técnicas previstas no edital.

8.4. A proposta deverá **discriminar os valores UNITÁRIOS E TOTAIS para cada item**, e incluir todas as despesas com encargos fiscais, comerciais, sociais e trabalhistas, e outros pertinentes ao objeto licitado.

8.5. Após a apresentação da proposta não cabe desistência, salvo por motivo justo decorrente de fato superveniente.

8.6. O preço inicial proposto será de exclusiva responsabilidade da Licitante, não lhe assistindo o direito de pleitear qualquer alteração dos mesmos, sob alegação de erro, omissão ou qualquer outro pretexto.

8.7. O prazo de validade das propostas apresentadas nesta licitação será, automaticamente, de 60 (sessenta) dias, contados da data fixada para a abertura das propostas, o qual, se necessário, poderá ser prorrogado mediante concordância dos Licitantes.

8.8. Para efeitos deste edital, poderão ser desclassificadas as propostas que forem manifestamente superfaturadas.

Parágrafo único: para análise do sobrepreço indicado acima, serão desclassificadas, antes da fase de lances, propostas que superarem em mais de 100% (cem pro cento) a média das cinco menores ofertas válidas.

9. DA SESSÃO DO PREGÃO

9.1. A partir do horário previsto no Edital, terá início a sessão pública do pregão eletrônico, com a divulgação das propostas de preços recebidas e em perfeita consonância com as especificações e condições de fornecimento detalhadas pelo edital.

9.2. OS LANCES SERÃO PELO VALOR TOTAL DO CONTRATO

9.3. Somente poderá participar da rodada de lances a licitante que anteriormente tenha cadastrado proposta de preços.

9.4. Aberta a etapa competitiva, será considerado como primeiro lance a proposta inicial de menor valor. Em seguida, os licitantes poderão encaminhar lances exclusivamente por meio eletrônico, sendo o licitante imediatamente informado de seu recebimento e respectivo horário de registro e valor.

9.5. Só serão aceitos lances cujos valores forem inferiores ao último lance que tenha sido anteriormente registrado no sistema pelo próprio licitante.

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

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

9.8. A etapa de lances da sessão pública será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema eletrônico, após o que transcorrerá o período de tempo de até 30 (trinta) minutos, aleatoriamente, determinado também pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

9.9. O sistema informará a proposta melhor classificada imediatamente após o encerramento da etapa de lances, quando for o caso, após negociação e decisão pelo pregoeiro acerca da aceitação da oferta.

9.10. **Para análise da aceitabilidade da proposta, a licitante deverá incluir em campo próprio do sistema os valores atualizados.**

9.11. A proposta final atualizada deverá ser encaminhada junto aos documentos de habilitação e conter a identificação da proponente, a assinatura de seu responsável legal, endereço, telefone, e-mail e nome do contato entre a licitante e o CRCRS.

9.12. Se a proposta ou o lance melhor classificado não for aceitável, ou se o fornecedor desatender às exigências habilitatórias, o pregoeiro examinará a proposta ou o lance subsequente, verificando a sua compatibilidade e a habilitação do participante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda o edital. Também nesta etapa o pregoeiro poderá negociar com o participante para que seja obtido melhor preço.

9.13. Constando o atendimento das exigências fixadas no Edital, o objeto será adjudicado ao autor da proposta ou lance de melhor preço.

9.14. No caso de desconexão com pregoeiro, no decorrer da etapa competitivas do certame, o sistema eletrônico poderá permanecer acessível aos licitantes para recepção de lances, retomando o pregoeiro, quando possível, sua atuação no Pregão, sem prejuízos dos atos realizados.

9.15. No caso de desconexão por tempo superior a 10 (dez) minutos, a sessão do pregão será suspensa, sendo reiniciada somente após comunicação expressa aos participantes.

10. DOS RECURSOS

10.1 – Dos atos relacionados com o pregão o recurso dependerá de manifestação do licitante ao final da sessão pública, dentro do prazo determinado pelo pregoeiro, manifestando sua intenção, com motivação simples, sendo-lhes facultado juntar memoriais relacionados à intenção manifestada no prazo de 03 (três) dias, ficando os demais licitantes, desde logo, intimados para apresentar contrarrazões em igual número de dias, que começarão a ser contados ao término daquele prazo.

10.2 – O recurso contra decisão do pregoeiro não terá efeito suspensivo e o seu acolhimento importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

10.3 – A falta de manifestação imediata importará a preclusão do direito de recurso.

10.4 – Não serão aceitos como recursos as alegações e memoriais que não se relacionem às razões indicadas pelo licitante na sessão pública.

10.5 – Os recursos e contrarrazões de recursos, deverão ser dirigidos ao Pregoeiro e registrados no Protocolo Geral do CRCRS, localizado na Avenida Praia de Belas, 1.554, em Porto Alegre/RS, de 2.ª a 6.ª feira, das 8h30min às 17h30min.

10.6 – Decididos os recursos e constatada a regularidade dos atos procedimentais, a autoridade competente homologará a adjudicação para determinar a contratação.

11. HABILITAÇÃO

11.1. São documentos necessários à habilitação:

a) Certidão Comprovando regularidade para com a Fazenda Federal e INSS;

b) Certidão comprovando a regularidade para com a Fazenda Estadual;

c) Certidão comprovando a regularidade para com a Fazenda Municipal;

d) Certidão comprovando a regularidade para com o FGTS;

e) Comprovante de inscrição no CNPJ;

f) **DECLARAÇÃO** da proponente de que não pesa contra si declaração de INIDONEIDADE expedida por órgão da ADMINISTRAÇÃO PÚBLICA de qualquer esfera;

g) **Certidão da DRT (Delegacia Regional do Trabalho)** ou **Declaração** de que cumpre o disposto no inciso XXXIII do art. 7º da Constituição Federal;

h) Ato constitutivo, Estatuto ou Contrato Social e alterações em vigor, devidamente registrados na Junta Comercial, ou alteração consolidada, quando sociedades comerciais e, no caso de sociedade por ações, acompanhadas de posse e nomeação de seus administradores, ou Registro comercial, no caso de empresa individual;

i) CERTIDÃO SIMPLIFICADA da Junta Comercial;

k) Prova de Inscrição no Cadastro de Contribuintes MUNICIPAL **e** ESTADUAL;

l) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa (CNDT), nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452 de 1º de maio de 1943;

m) **Declaração**, sob as penas da lei, de que cumpre os requisitos legais para a qualificação como ME ou EPP;

n) Atestados de capacidade técnica e operacional, que comprovem aptidão para execução do objeto da presente licitação, emitidos por pessoas jurídicas de direito público ou privado que tenham contratado junto a ofertante:

I – Ao menos um atestado comprovando a comercialização de **lote de licenças** de qualquer software.

II – Ao menos um atestado, comprovando a realização de serviço de instalação, treinamento e manutenção de solução antivírus.

11.2. Caso a licitante possua CERTIFICADO de Registro Cadastral – CRC, emitido pela CELIC, pode apresentá-lo, ficando dispensada a apresentação dos documentos relativos às informações válidas já atestadas pelo referido certificado.

11.3. Os documentos que não possuírem prazo de validade somente serão aceitos com data não excedente a 90 (noventa) dias de antecedência da data prevista para a apresentação das propostas.

11.4. Os documentos devem ser apresentados em original ou cópia autenticada. Os documentos apresentados em original poderão ser restituídos à licitante mediante apresentação de cópia, que será autenticada pelo CRCRS.

11.5. O prazo para entrega da documentação será de DOIS DIAS ÚTEIS após a sessão pública.

12. DA ADJUDICAÇÃO

12.1 – Após a análise da documentação de habilitação recebida na sede do CRCRS, será efetuada a adjudicação do lote em questão.

12.2 – Em caso de não adjudicação constará a justificativa da mesma no Sistema de Compras On-line do Banrisul, além de citado na ata eletrônica.

13. DAS PENALIDADES

A licitante que, convocada, recusar-se a firmar o contrato ou não comprovar o atendimento às condições de habilitação no prazo consignado, sujeitar-se-á a penalidade relativa à rescisão contratual por culpa da contratada, sem prejuízo da penalidade cominada no art. 28 do Decreto 5.450/05.

14. DISPOSIÇÕES FINAIS

14.1 – Todos os eventos ocorridos durante a sessão pública de disputa serão registrados e publicados, em ata eletrônica, imediatamente após o término da disputa, tornando-se disponível ao acesso por qualquer cidadão.

14.1.1 – A ata poderá ser acessada pela pesquisa de licitações disponibilizada para o público em geral no Portal de Compras como também pela pesquisa na área de acesso restrito. Ambas publicam o mesmo conteúdo.

14.1.2 – Os demais atos licitatórios serão registrados no processo da licitação.

14.2 – A Licitante deverá examinar detidamente as disposições contidas neste Edital e seus anexos, pois a simples apresentação da proposta de preços e da documentação de habilitação submete a licitante à aceitação incondicional de seus termos, bem como representa o conhecimento integral do objeto em licitação, não sendo aceita alegação de desconhecimento de qualquer pormenor.

14.3 – o CRCRS reserva a si o direito de revogar a presente licitação por razões de interesse público ou anulá-la, no todo ou em parte, por vício ou ilegalidade, bem como prorrogar o prazo para recebimento e/ou abertura da proposta de preços.

14.4 – é facultado ao pregoeiro, em qualquer fase do pregão, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo, vedada à licitante a inclusão posterior de documento ou informação que deveria constar originalmente da proposta de preços ou da documentação de habilitação.

14.5 – O desatendimento de exigências formais não essenciais não importará no afastamento da Licitante, desde que sejam possíveis a aferição de sua qualificação e a exata compreensão da sua proposta, durante a realização da audiência pública do pregão. As normas que disciplinam este pregão serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento da segurança da futura contratação.

14.6 – O CRCRS reserva-se o direito de aceitar total ou parcialmente quaisquer propostas, ou a todas rejeitar sem que caiba a proponente qualquer direito a indenização ou ressarcimento.

14.7 – Da mesma forma, o CRCRS reserva-se o direito de contratar total ou parcialmente os itens solicitados, sem que caiba a proponente qualquer direito a indenização ou ressarcimento.

Porto Alegre, 15 de dezembro de 2016.

Cauê Ardenghi Biedacha
Coordenador da Seção de Compras e Suprimentos

PREGÃO ELETRÔNICO CRCRS 15/2016

PROCESSO ADMINISTRATIVO 104/2016

ANEXO I

TERMO DE REFERÊNCIA

1. BASE LEGAL

Este documento foi elaborado com base na Lei nº 10.520/02, Decreto nº 5.450/05, Lei Complementar 123/06 e Lei nº 8.666/93, constituindo peça integrante do instrumento convocatório.

1. OBJETO

O objeto da presente Licitação é a aquisição de licenças de Software Antivírus com fornecimento de 180 licenças para estações de trabalho, dispositivos móveis e servidores, incluindo instalação, configuração e serviço de suporte “ON SITE” durante os primeiros 180 dias, contados da implementação, contemplando atualizações do banco de dados de ameaças, por um período de 3 anos.

2. JUSTIFICATIVA DA CONTRATAÇÃO

A crescente demanda de serviços inerentes às atividades do CRCRS exige uma constante adequação tecnológica visando proteger e manter a qualidade dos serviços prestados.

De acordo com a norma internacional ISO IEC 27001:2006, que trata da certificação para Sistemas de Gestão de Segurança de Informação, da qual citamos três atributos básicos relativos a informação: confidencialidade, integridade e disponibilidade, atributos estes que a Seção de TI de acordo com suas atribuições institucionais promove e mantém ações que permitam o CRCRS identificar, analisar e qualificar riscos que possam comprometer tais atributos.

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

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

3. DESCRIÇÃO DO OBJETO

3.1. **180 (cento e oitenta)** licenças de software de proteção contra vírus de computador e outros códigos maliciosos.

3.2. A licitante deverá fornecer uma solução completa e integrada de um único fabricante que inclua todos os produtos abaixo relacionados.

3.3. Todos os produtos oferecidos devem ser referentes às últimas versões disponíveis do fabricante.

3.4. Serão aceitos para efeito de comprovação documentos, manuais, ou declarações cuja origem seja exclusivamente do fabricante dos produtos.

3.5. Licenças contemplando atualizações do banco de dados de ameaças por um período de atualizações da solução por **36 (trinta e seis) meses**.

4 ESPECIFICAÇÕES TÉCNICAS - REQUISITOS MÍNIMOS

4.1 Servidor de Administração e Console Administrativa

4.1.1 Compatibilidade

4.1.1.1 Microsoft Windows Server 2003 ou superior (Todas edições)
4.1.1.2 Microsoft Windows Server 2003 x64 ou superior (Todas edições)
4.1.1.3 Microsoft Windows Server 2008 (Todas edições)
4.1.1.4 Microsoft Windows Server 2008 Core (Todas edições)
4.1.1.5 Microsoft Windows Server 2008 x64 SP1 (Todas edições)
4.1.1.6 Microsoft Windows Server 2008 R2 (Todas edições)
4.1.1.7 Microsoft Windows Server 2008 R2 Core (Todas edições)
4.1.1.8 Microsoft Windows Server 2012 (Todas edições)
4.1.1.9 Microsoft Windows Server 2012 R2 (Todas edições)
4.1.1.10 Microsoft Windows XP Professional SP2 ou superior
4.1.1.11 Microsoft Windows XP Professional x64 e superior
4.1.1.12 Microsoft Windows Vista SP1
4.1.1.13 Microsoft Windows Vista x64 SP1
4.1.1.14 Microsoft Windows 7
4.1.1.15 Microsoft Windows 7 x64
4.1.1.16 Microsoft Windows 8
4.1.1.17 Microsoft Windows 8 x64
4.1.1.18 Suporta as seguintes plataformas virtuais
4.1.1.19 VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5
4.1.1.20 Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2
4.1.1.21 KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS

4.1.1.22 Microsoft VirtualPC 6.0.156.0
4.1.1.23 Parallels Desktop 7 e superior
4.1.1.24 Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado)
4.1.1.25 Citrix XenServer 6.1, 6.2

4.1.2 Características:

4.1.2.1 A console deve ser acessada via WEB (HTTPS) ou MMC;
4.1.2.2 Console deve ser baseada no modelo cliente/servidor
4.1.2.3 Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade
4.1.2.4 Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.
4.1.2.5 Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM
4.1.2.6 As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos;
4.1.2.7 Capacidade de remover remotamente e automaticamente 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;
4.1.2.8 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;
4.1.2.9 Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria
4.1.2.10 A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas
4.1.2.11 Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador
4.1.2.12 Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows
4.1.2.13 Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
4.1.2.14 A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle
4.1.2.15 Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por sub-rede com os seguintes parâmetros: KB/s e horário.

4.1.2.16 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução anti-vírus;

4.1.2.17 Capacidade de gerenciar smartphones e tablets (Windows Phone , Android e iOS) protegidos pela solução anti-vírus;

4.1.2.18 Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto;

4.1.2.19 Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

4.1.2.20 Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de anti-vírus para que seja instalado nas máquinas clientes;

4.1.2.21 A comunicação entre o cliente e o servidor de administração deve ser criptografada.

4.1.2.22 Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

4.1.2.23 Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado através dos seguintes parâmetros:

Nome do computador

Nome do domínio

Range de IP

Sistema Operacional

Máquina virtual

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

4.1.2.25 Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional

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

4.1.2.27 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;

4.1.2.28 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;

4.1.2.29 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;

4.1.2.30 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;
4.1.2.31 Deve fornecer as seguintes informações dos computadores:
4.1.2.32 Se o antivírus está instalado;
4.1.2.33 Se o antivírus está iniciado;
4.1.2.34 Se o antivírus está atualizado;
4.1.2.35 Minutos/horas desde a última conexão da máquina com o servidor administrativo;
4.1.2.36 Minutos/horas desde a última atualização de vacinas
4.1.2.37 Data e horário da última verificação executada na máquina;
4.1.2.38 Versão do antivírus instalado na máquina;
4.1.2.39 Se é necessário reiniciar o computador para aplicar mudanças;
4.1.2.40 Data e horário de quando a máquina foi ligada;
4.1.2.41 Quantidade de vírus encontrados (contador) na máquina;
4.1.2.42 Nome do computador;
4.1.2.43 Domínio ou grupo de trabalho do computador;
4.1.2.44 Data e horário da última atualização de vacinas;
4.1.2.45 Sistema operacional com Service Pack;
4.1.2.46 Quantidade de processadores;
4.1.2.47 Quantidade de memória RAM;
4.1.2.48 Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
4.1.2.49 Endereço IP;
4.1.2.50 Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.
4.1.2.51 Atualizações do Windows Updates instaladas
4.1.2.52 Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de audio, adaptadores de rede, monitores, drives de CD/DVD
4.1.2.53 Vulnerabilidades de aplicativos instalados na máquina
4.1.2.54 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterará-las;
4.1.2.55 Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
4.1.2.56 Mudança de gateway;
4.1.2.57 Mudança de subnet DNS;
4.1.2.58 Mudança de domínio;
4.1.2.59 Mudança de servidor DHCP;
4.1.2.60 Mudança de servidor DNS;
4.1.2.61 Mudança de servidor WINS;
4.1.2.62 Aparecimento de nova subnet;
4.1.2.63 Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
4.1.2.64 Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

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

4.1.2.66 Capacidade de herança de tarefas e políticas na estrutura hierarquica de servidores administrativos;

4.1.2.67 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;

4.1.2.68 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.

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

4.1.2.70 Capacidade de gerar traps SNMP para monitoramento de eventos;

4.1.2.71 Capacidade de enviar e-mails para contas específicas em caso de algum evento;

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

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

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

4.1.2.75 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;

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

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

4.1.2.78 Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

Nome do vírus

Nome do arquivo infectado

Data e hora da detecção

Nome da máquina ou endereço IP

Ação realizada

4.1.2.79 Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

4.1.2.80 Capacidade de realizar inventário de hardware de todas as máquinas clientes;

4.1.2.81 Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
4.1.2.82 Capacidade de diferenciar máquinas virtuais de máquinas físicas;

4.2 Estações Windows

4.2.1 Compatibilidade:

4.2.1.1 Microsoft Windows XP Professional SP3 e superior
4.2.1.2 Microsoft Windows Vista Business/Enterprise/Ultimate SP2
4.2.1.3 Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2
4.2.1.4 Microsoft Windows 7 Professional/Enterprise/Ultimate
4.2.1.5 Microsoft Windows 7 Professional/Enterprise/Ultimate x64
4.2.1.6 Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 e superior
4.2.1.7 Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1 e superior
4.2.1.8 Microsoft Windows 8 Professional/Enterprise
4.2.1.9 Microsoft Windows 8 Professional/Enterprise x64
4.2.1.10 Microsoft Windows 8.1 Enterprise x86 / 64
4.2.1.11 Microsoft Windows 8.1 Pro x86 /64
4.2.1.12 Microsoft Windows 10 Enterprise x86 / 64
4.2.1.13 Microsoft Windows 10 Pro x86 / 64

4.2.2 Características:

4.2.2.1 Deve prover as seguintes proteções:
4.2.2.2 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
4.2.2.3 Antivírus de Web (módulo para verificação de sites e downloads contra vírus)
4.2.2.4 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos)
4.2.2.5 Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas)
4.2.2.6 O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza
4.2.2.7 Firewall com IDS
4.2.2.8 Autoproteção (contra ataques aos serviços/processos do antivírus)
4.2.2.9 Controle de dispositivos externos
4.2.2.10 Controle de acesso a sites por categoria
4.2.2.11 Controle de acesso a sites por horário
4.2.2.12 Controle de acesso a sites por usuários
4.2.2.13 Controle de execução de aplicativos

4.2.2.14 Controle de vulnerabilidades do Windows e dos aplicativos instalados

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

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

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

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

4.2.2.19 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

4.2.2.20 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;

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

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

4.2.2.23 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;

4.2.2.24 Capacidade de verificar somente arquivos novos e alterados;

4.2.2.25 Capacidade de verificar objetos usando heurística;

4.2.2.26 Capacidade de agendar uma pausa na verificação;

4.2.2.27 Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias

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

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

4.2.2.30 Perguntar o que fazer, ou;

4.2.2.31 Bloquear acesso ao objeto;

4.2.2.32 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);

4.2.2.33 Caso positivo de desinfecção:

4.2.2.34 Restaurar o objeto para uso;
4.2.2.35 Caso negativo de desinfecção:
4.2.2.36 Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);
4.2.2.37 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
4.2.2.38 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);
4.2.2.39 Capacidade de verificar tráfego de MSN, IRC, etc, contra vírus e links phishings;
4.2.2.40 Capacidade de verificar links inseridos em e-mails contra phishings;
4.2.2.41 Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Opera;
4.2.2.42 Capacidade de verificação de corpo e anexos de e-mails usando heurística;
4.2.2.43 O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
4.2.2.44 Perguntar o que fazer, ou;
4.2.2.45 Bloquear o e-mail;
4.2.2.46 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);
4.2.2.47 Caso positivo de desinfecção:
4.2.2.48 Restaurar o e-mail para o usuário;
4.2.2.49 Caso negativo de desinfecção:
4.2.2.50 Mover para quarentena ou apagar o objeto (de acordo com a configuração preestabelecida pelo administrador);
4.2.2.51 Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.
4.2.2.52 Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.
4.2.2.53 Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.
4.2.2.54 Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
4.2.2.55 Deve ter suporte total ao protocolo IPv6;
4.2.2.56 Capacidade de alterar as portas monitoradas pelos módulos de Web e e-mail;
4.2.2.57 Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
4.2.2.58 Perguntar o que fazer, ou;
4.2.2.59 Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
4.2.2.60 Permitir acesso ao objeto;

4.2.2.61 O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
4.2.2.62 Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou;
4.2.2.63 Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.
4.2.2.64 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.
4.2.2.65 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 em parceria com as vacinas.
4.2.2.66 Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.
4.2.2.67 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.
4.2.2.68 Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).
4.2.2.69 Capacidade de distinguir diferentes sub-nets e conceder opção de ativar ou não o firewall para uma sub-net específica;
4.2.2.70 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 junto as vacinas.
4.2.2.71 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
4.2.2.72 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
4.2.2.73 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 à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
4.2.2.74 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
4.2.2.75 Discos de armazenamento locais
4.2.2.76 Armazenamento removível
4.2.2.77 Impressoras
4.2.2.78 CD/DVD
4.2.2.79 Modems
4.2.2.80 Dispositivos multifuncionais

4.2.2.81 Leitores de smart card
4.2.2.82 Wi-Fi
4.2.2.83 Adaptadores de rede externos
4.2.2.84 Dispositivos MP3 ou smartphones
4.2.2.85 Dispositivos Bluetooth
4.2.2.86 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.
4.2.2.87 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.
4.2.2.88 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.
4.2.2.89 Capacidade de configurar novos dispositivos por Class ID/Hardware ID
4.2.2.90 Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, audio, etc), com possiibilidade de configuração por usuário ou grupos de usuários e agendamento.
4.2.2.91 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).
4.2.2.92 Capacidade de bloquear execução de aplicativo que está em armazenamento externo.
4.2.2.93 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.
4.2.2.94 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.
4.2.2.95 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.

4.3 Estações e Servidores Mac OS

4.3.1 Compatibilidade:

4.3.1.1 Mac OS X 10.4.11 ou superior
4.3.1.2 Mac OS X 10.5 (Leopard)
4.3.1.3 Mac OS X 10.6 (Snow Leopard)
4.3.1.4 Mac OS X 10.7 (Lion)
4.3.1.5 Mac OS X 10.8 (Mountain Lion)
4.3.1.6 Mac OS X 10.9 (Mavericks)
4.3.1.7 Mac OS X 10.10 (Yosemite)

4.3.1.8 Mac OS X Server 10.6 x86 e x64
4.3.1.9 Mac OS X Server 10.7 x86 e x64

4.3.2 Características:

4.3.2.1 Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
4.3.2.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
4.3.2.3 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;
4.3.2.4 Deve possuir suportes a notificações utilizando o Growl;
4.3.2.5 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independente do nível das ameaças encontradas no período (alta, média ou baixa).
4.3.2.6 Capacidade de voltar para a base de dados de vacina anterior;
4.3.2.7 Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
4.3.2.8 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;
4.3.2.9 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
4.3.2.10 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;
4.3.2.11 Capacidade de verificar somente arquivos novos e alterados;
4.3.2.12 Capacidade de verificar objetos usando heurística;
4.3.2.13 Capacidade de agendar uma pausa na verificação;
4.3.2.14 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
4.3.2.15 Perguntar o que fazer, ou;
4.3.2.16 Bloquear acesso ao objeto;
4.3.2.17 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
4.3.2.18 Caso positivo de desinfecção:
4.3.2.19 Restaurar o objeto para uso;

4.3.2.20 Caso negativo de desinfecção:
4.3.2.21 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
4.3.2.22 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
4.3.2.23 Capacidade de verificar arquivos de formato de e-mail;
4.3.2.24 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;
4.3.2.25 Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento;
4.3.2.26 Estações de trabalho Linux –
4.3.2.27 Compatibilidade:
4.3.2.28 Plataforma 32-bits:
4.3.2.29 Red Hat Enterprise Linux 5.8 Desktop
4.3.2.30 Red Hat Enterprise Linux 6.2 Desktop
4.3.2.31 Fedora 16
4.3.2.32 CentOS-6.2
4.3.2.33 SUSE Linux Enterprise Desktop 10 SP4
4.3.2.34 SUSE Linux Enterprise Desktop 11 SP2
4.3.2.35 openSUSE Linux 12.1
4.3.2.36 openSUSE Linux 12.2
4.3.2.37 Debian GNU/Linux 6.0.5
4.3.2.38 Mandriva Linux 2011
4.3.2.39 Ubuntu 10.04 LTS
4.3.2.40 Ubuntu 12.04 LTS
4.3.2.41 Plataforma 64-bits:
4.3.2.42 Red Hat Enterprise Linux 5.8
4.3.2.43 Red Hat Enterprise Linux 6.2 Desktop
4.3.2.44 Fedora 16
4.3.2.45 CentOS-6.2
4.3.2.46 SUSE Linux Enterprise Desktop 10 SP4
4.3.2.47 SUSE Linux Enterprise Desktop 11 SP2
4.3.2.48 openSUSE Linux 12.1
4.3.2.49 openSUSE Linux 12.2
4.3.2.50 Debian GNU/Linux 6.0.5
4.3.2.51 Ubuntu 10.04 LTS
4.3.2.52 Ubuntu 12.04 LTS
4.3.2.53 Características:
4.3.2.54 Deve prover as seguintes proteções:
4.3.2.55 Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
4.3.2.56 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
4.3.2.57 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

4.3.2.58 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
4.3.2.59 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;
4.3.2.60 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
4.3.2.61 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
4.3.2.62 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
4.3.2.63 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
4.3.2.64 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;
4.3.2.65 Capacidade de verificar objetos usando heurística;
4.3.2.66 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
4.3.2.67 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
4.3.2.68 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
4.3.2.69
4.3.2.70 Servidores Windows –
4.3.2.71 Compatibilidade:
4.3.2.72 Microsoft Windows Server 2003 Standard/Enterprise SP2 x86/x64
4.3.2.73 Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 x86/x64
4.3.2.74 Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1 x86/x64
4.3.2.75 Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 x86/x64
4.3.2.76 Microsoft Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1
4.3.2.77 Microsoft Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1
4.3.2.78 Microsoft Windows Server 2012 Foundation/Essentials/Standard x64

4.3.2.79 Microsoft Windows Hyper-V Server 2008 R2 SP1
4.3.2.80 Microsoft Terminal baseado em Windows Server 2003
4.3.2.81 Microsoft Terminal baseado em Windows Server 2008
4.3.2.82 Microsoft Terminal baseado em Windows Server 2008 R2
4.3.2.83 Características:
4.3.2.84 Deve prover as seguintes proteções:
4.3.2.85 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
4.3.2.86 Auto-proteção contra ataques aos serviços/processos do antivírus
4.3.2.87 Firewall com IDS
4.3.2.88 Controle de vulnerabilidades do Windows e dos aplicativos instalados
4.3.2.89 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
4.3.2.90 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
4.3.2.91 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
4.3.2.92 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
4.3.2.93 Gerenciamento de tarefa (criar ou excluir tarefas de verificação)
4.3.2.94 Leitura de configurações
4.3.2.95 Modificação de configurações
4.3.2.96 Gerenciamento de Backup e Quarentena
4.3.2.97 Visualização de relatórios
4.3.2.98 Gerenciamento de relatórios
4.3.2.99 Gerenciamento de chaves de licença
4.3.2.100 Gerenciamento de permissões (adicionar/excluir permissões acima)
4.3.2.101 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
4.3.2.102 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
4.3.2.103 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 à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
4.3.2.104 Capacidade de separadamente selecionar o número de processos que executarão funções de varredura em tempo real, o número de processos que executarão a varredura sob-demanda e o número máximo de processos que podem ser executados no total.

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

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

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

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

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

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

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

4.3.2.112 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

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

4.3.2.114 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;

4.3.2.115 Capacidade de verificar somente arquivos novos e alterados;

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

4.3.2.117 Capacidade de verificar objetos usando heurística;

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

4.3.2.119 Capacidade de agendar uma pausa na verificação;

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

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

4.3.2.122 Perguntar o que fazer, ou;

4.3.2.123 Bloquear acesso ao objeto;

4.3.2.124 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);

4.3.2.125 Caso positivo de desinfecção:
4.3.2.126 Restaurar o objeto para uso;
4.3.2.127 Caso negativo de desinfecção:
4.3.2.128 Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);
4.3.2.129 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
4.3.2.130 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
4.3.2.131 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
4.3.2.132 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

4.4 Servidores Linux

4.4.1 Compatibilidade:

4.4.1.1 Plataforma 32-bits:
4.4.1.2 Red Hat Enterprise Linux 6.2 Server;
4.4.1.3 Red Hat Enterprise Linux 5.8 Server
4.4.1.4 Fedora 16;
4.4.1.5 CentOS-6.2;
4.4.1.6 SUSE Linux Enterprise Server 11 SP2;
4.4.1.7 openSUSE Linux 12.1;
4.4.1.8 openSUSE Linux 12.2;
4.4.1.9 Mandriva Enterprise Server 5.2;
4.4.1.10 Ubuntu Server 10.04.2 LTS;
4.4.1.11 Ubuntu Server 12.04 LTS;
4.4.1.12 Debian GNU/Linux 6.0.5;
4.4.1.13 Plataforma 64-bits:
4.4.1.14 Red Hat Enterprise Linux 6.2 Server;
4.4.1.15 Red Hat Enterprise Linux 5.8 Server
4.4.1.16 Fedora 16;
4.4.1.17 CentOS-6.2;
4.4.1.18 SUSE Linux Enterprise Server 11 SP2;
4.4.1.19 openSUSE Linux 12.1;
4.4.1.20 openSUSE Linux 12.2;
4.4.1.21 Mandriva Enterprise Server 5.2;
4.4.1.22 Ubuntu Server 10.04.2 LTS;
4.4.1.23 Ubuntu Server 12.04 LTS;
4.4.1.24 Debian GNU/Linux 6.0.5;

4.4.2 Características:

4.4.2.1 Deve prover as seguintes proteções:

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

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

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

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

4.4.2.6 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;

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

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

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

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

4.4.2.11 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;

4.4.2.12 Capacidade de verificar objetos usando heurística;

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

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

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

4.5 Smartphones e tablets

4.5.1 Compatibilidade:

4.5.1.1 Apple iOS 7.0 – 9.2

4.5.1.2 Windows Phone 8.1

4.5.1.3 Android OS 2.3 – 5.1

4.5.2 Características:

4.5.2.1 Deve prover as seguintes proteções:
4.5.2.2 Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
4.5.2.3 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.
4.5.2.4 Arquivos abertos no smartphone
4.5.2.5 Programas instalados usando a interface do smartphone
4.5.2.6 Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
4.5.2.7 Deverá isolar em área de quarentena os arquivos infectados;
4.5.2.8 Deverá atualizar as bases de vacinas de modo agendado;
4.5.2.9 Deverá bloquear spams de SMS através de Black lists;
4.5.2.10 Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;
4.5.2.11 Capacidade de desativar por política:
Wi-fi
Camera
Bluetooth
4.5.2.12 Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.
4.5.2.13 Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha
4.5.2.14 Deverá ter firewall pessoal;
4.5.2.15 Capacidade de tirar fotos quando a senha for inserida incorretamente (Mugshot)
4.5.2.16 Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1
4.5.2.17 Capacidade de enviar comandos remotamente de:
Localizar
Bloquear
4.5.2.18 Capacidade de detectar Jailbreak em dispositivos iOS
4.5.2.19 Capacidade de bloquear o acesso a site por categoria em dispositivos
4.5.2.20 Capacidade de bloquear o acesso a sites phishing ou malicioso
4.5.2.21 Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais
4.5.2.22 Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído
4.5.2.23 Capacidade de configurar White e blacklist de aplicativos
4.5.2.24 Capacidade de localizar o dispositivo quando necessário
4.5.2.25 Permitir atualização das definições quando estiver em “roaming”

4.5.2.26 Capacidade de selecionar endereço do servidor para buscar a definição de vírus
4.5.2.27 Capacidade de enviar URL de instalação por e-mail
4.5.2.28 Capacidade de fazer a instalação através de um link QRCode
4.5.2.29 Capacidade de executar as seguintes ações caso a desinfecção falhe:
Deletar
4.5.2.30 Ignorar
4.5.2.31 Quarentena
Gerenciamento de dispositivos móveis (MDM):
4.5.2.32 Compatibilidade:
4.5.2.33 Dispositivos conectados através do Microsoft Exchange ActiveSync
4.5.2.34 Apple iOS
4.5.2.35 Windows Phone
4.5.2.36 Android
4.5.2.37 Dispositivos com suporte ao Apple Push Notification (APNs) service
4.5.2.38 Apple iOS 3.0 ou superior
4.5.2.39 Características:
4.5.2.40 Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange
4.5.2.41 Capacidade de ajustar as configurações de:
4.5.2.42 Sincronização de e-mail
4.5.2.43 Uso de aplicativos
4.5.2.44 Senha do usuário
4.5.2.45 Criptografia de dados
4.5.2.46 Conexão de mídia removível
4.5.2.47 Capacidade de instalar certificados digitais em dispositivos móveis
4.5.2.48 Capacidade de, remotamente, resetar a senha de dispositivos iOS
4.5.2.49 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS
4.5.2.50 Capacidade de, remotamente, bloquear um dispositivo iOS

4.6 Criptografia:

4.6.1 Compatibilidade:

4.6.1.1 Microsoft Windows XP Professional SP3 ou superior
4.6.1.2 Microsoft Windows Vista Business/Enterprise/Ultimate SP2
4.6.1.3 Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2
4.6.1.4 Microsoft Windows 7 Professional/Enterprise/Ultimate
4.6.1.5 Microsoft Windows 7 Professional/Enterprise/Ultimate x64
4.6.1.6 Microsoft Windows 8 Professional/Enterprise

4.6.1.7 Microsoft Windows 8 Professional/Enterprise x64
4.6.1.8 Microsoft Windows 8.1 Professional / Enterprise
4.6.1.9 Microsoft Windows 8.1 Professional / Enterprise x64
4.6.1.10 Microsoft Windows 10 Pro x86 / x64
4.6.1.11 Microsoft Windows 10 Enterprise x86 /x64

4.6.2 Características:

4.6.2.1 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.
4.6.2.2 Utilizar, no mínimo, algoritmo AES com chave de 256 bits.
4.6.2.3 Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário.
4.6.2.4 Capacidade de utilizar Single Sign-On para a autenticação de pré-boot.
4.6.2.5 Permitir criar vários usuários de autenticação pré-boot.
4.6.2.6 Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento.
4.6.2.7 Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
4.6.2.8 Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes.
4.6.2.9 Criptografar todos os arquivos individualmente.
4.6.2.10 Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas.
4.6.2.11 Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha.
4.6.2.12 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.
4.6.2.13 Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados.
4.6.2.14 Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados.
4.6.2.15 Verifica compatibilidade de hardware antes de aplicar a criptografia
4.6.2.16 Possibilita estabelecer parâmetros para a senha de criptografia
4.6.2.17 Bloqueia o reuso de senhas
4.6.2.18 Bloqueia a senha após um número de tentativas pré estabelecidas

4.6.2.19 Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante *templates* customizados

4.6.2.20 Permite criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo

4.6.2.21 Permite criptografar as seguintes pastas pré-definidas: "meus documentos", "Favoritos", "Desktop", "Arquivos temporários" e "Arquivos do outlook"

4.6.2.22 Permite utilizar variáveis de ambiente para criptografar pastas customizadas.

4.6.2.23 Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc

4.6.2.24 Permite criar um grupo de extensões de arquivos a serem criptografados

4.6.2.25 Capacidade de criar regra de criptografia para arquivos gerados por aplicações

4.6.2.26 Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

4.7 Gerenciamento de Sistemas:

4.7.1 Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal.

4.7.2 Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis.

4.7.3 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.

4.7.4 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.

4.7.5 Capacidade de gerenciar licenças de softwares de terceiros.

4.7.6 Capacidade de registrar mudanças de hardware nas máquinas gerenciadas.

4.7.7 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.

4.7.8 Possibilita fazer distribuição de software de forma manual e agendada

4.7.9 Suporta modo de instalação silenciosa

4.7.10 Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis

4.7.11 Possibilita fazer a distribuição através de agentes de atualização

4.7.12 Utiliza tecnologia multicast para evitar tráfego na rede

4.7.13 Possibilita criar um inventário centralizado de imagens

4.7.14 Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário

4.7.15 Suporte a WakeOnLan para deploy de imagens

4.7.16 Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches

4.7.17 Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento

4.7.18 Capacidade de gerar relatórios de vulnerabilidades e patches

4.7.19 Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração

4.7.20 Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador

4.7.21 Permite baixar atualizações para o computador sem efetuar a instalação

4.7.22 Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas

4.7.23 Capacidade de instalar correções de vulnerabilidades de acordo com a severidade

4.7.24 Permite selecionar produtos a serem atualizados pela console de gerenciamento

4.7.25 Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc

4.8 Servidores de e-mail Windows

4.8.1 Compatibilidade:

4.8.1.1 Microsoft Essential Business Server 2008 Standard
4.8.1.2 Microsoft Essential Business Server 2008 Premium
4.8.1.3 Microsoft Windows Server 2008 x64 R2 Enterprise Edition
4.8.1.4 Microsoft Windows Server 2008 x64 R2 Standard Edition
4.8.1.5 Microsoft Windows Server 2008 x64 Enterprise Edition SP1
4.8.1.6 Microsoft Windows Server 2008 x64 Enterprise Edition SP2
4.8.1.7 Microsoft Windows Server 2008 x64 Standard Edition SP1

4.8.1.8 Microsoft Windows Server 2008 x64 Standard Edition SP2
4.8.1.9 Microsoft Windows Server 2003 x64 R2 Enterprise Edition SP2
4.8.1.10 Microsoft Windows Server 2003 x64 R2 Standard Edition SP2
4.8.1.11 Microsoft Windows Server 2003 x64 Enterprise Edition SP2
4.8.1.12 Microsoft Windows Server 2003 x64 Standard Edition SP2
4.8.1.13 Microsoft Exchange Server 2003 Standard Edition
4.8.1.14 Microsoft Exchange Server 2003 Enterprise Edition
4.8.1.15 Microsoft Exchange Server 2007 SP1 x64
4.8.1.16 Microsoft Exchange Server 2007 SP2 x64
4.8.1.17 Microsoft Exchange Server 2007 SP3 x64
4.8.1.18 Microsoft Exchange Server 2010
4.8.1.19 Microsoft Exchange Server 2010 SP1

4.8.2 Características:

4.8.2.1 Deve utilizar as tecnologias VSAPI 2.0, 2.5 e 2.6;
4.8.2.2 Capacidade de iniciar várias cópias do processo de antivírus;
4.8.2.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
4.8.2.4 Capacidade de verificar pastas públicas, e-mails enviados, recebidos e armazenados contra vírus, spywares, adwares, worms, trojans e riskwares;
4.8.2.5 Capacidade de verificar pastas públicas e e-mails armazenados de forma agendada, utilizando as últimas vacinas e heurística;
4.8.2.6 O antivírus, ao encontrar um objeto infectado, deve:
4.8.2.7 Desinfetar o objeto, notificando o recipiente, destinatário e administradores, ou
4.8.2.8 Excluir o objeto, substituindo-o por uma notificação;
4.8.2.9 Bloquear acesso ao objeto;
4.8.2.10 Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração preestabelecida pelo administrador);
4.8.2.11 Caso positivo de desinfecção:
4.8.2.12 Restaurar o objeto para uso;
4.8.2.13 Caso negativo de desinfecção:
4.8.2.14 Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);
4.8.2.15 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
4.8.2.16 Capacidade de enviar notificações sobre vírus detectados para o administrador, para o recipiente e remetente da mensagem infectada.
4.8.2.17 Capacidade de gravar logs de atividade de vírus nos eventos do sistema e nos logs internos da aplicação;

4.8.2.18 Capacidade de detectar disseminação em massa de e-mails infectados, informando o administrador e registrando tais eventos nos logs do sistema e da aplicação.

4.9 Servidores de e-mail Linux:

4.9.1 Compatibilidade:

4.9.1.1 Sistemas 32-bit:
4.9.1.2 Red Hat Enterprise Linux Server 5.2 Server
4.9.1.3 Fedora 9
4.9.1.4 SUSE Linux Enterprise Server 10 SP2
4.9.1.5 openSUSE Linux 11.0
4.9.1.6 Debian GNU/Linux 4.0 (r4)
4.9.1.7 Mandriva Corporate Server 4.0
4.9.1.8 Ubuntu 8.04.1 Server Edition
4.9.1.9 Sistemas 64-bit:
4.9.1.10 Fedora 9
4.9.1.11 Red Hat Enterprise Linux Server 5.2 Server
4.9.1.12 SUSE Linux Enterprise Server 10 SP2
4.9.1.13 openSUSE Linux 11.0
4.9.1.14 Debian 6.0.2
4.9.1.15 MTA:
4.9.1.16 Sendmail 8.12.x ou superior;
4.9.1.17 Qmail 1.03;
4.9.1.18 Postfix 2.x;
4.9.1.19 Exim 4.x;

4.9.2 Características:

4.9.2.1 Capacidade de verificar o tráfego SMTP do servidor contra malware em todos os elementos do e-mail: cabeçalho, corpo e anexo;
4.9.2.2 Capacidade de notificar o administrador, o remetente e o destinatário caso um arquivo malicioso seja encontrado no e-mail;
4.9.2.3 Capacidade de quarentenar objetos maliciosos;
4.9.2.4 Capacidade de salvar backup dos objetos antes de tentativa de desinfecção;
4.9.2.5 Capacidade de fazer varredura no sistema de arquivos do servidor;
4.9.2.6 Capacidade de filtrar anexos por nome ou tipo de arquivo;
4.9.2.7 Capacidade de criar grupos de usuários para aplicar regras de verificação de e-mails;
4.9.2.8 Deve permitir gerenciamento via console WEB;
4.9.2.9 Deve ser atualizado de maneira automática via internet ou por servidores locais, com frequência horária.

4.10 Servidores de gateway

4.10.1 Compatibilidade:

4.10.1.1 Microsoft Windows Server 2003 SP2 Standard/Enterprise
4.10.1.2 Microsoft Windows Server 2003 R2 SP2 Standard/Enterprise
4.10.1.3 Microsoft Windows Server 2008 x64 SP2 Standard/Enterprise
4.10.1.4 Microsoft Windows Server 2008 R2 x64 Standard/Enterprise
4.10.1.5 Microsoft ISA Server 2006 Standard/Enterprise
4.10.1.6 Microsoft Forefront Threat Management Gateway (TMG) 2012 Standard/Enterprise
4.10.1.7 Red Hat Enterprise Linux 5.4 Server
4.10.1.8 Red Hat Enterprise Linux Advanced Server 4 Update 4
4.10.1.9 Fedora 12
4.10.1.10 Fedora Core 6
4.10.1.11 SuSE Linux Enterprise Server 10 SP3
4.10.1.12 SuSE Linux Enterprise Server 11
4.10.1.13 SuSE Linux Enterprise Desktop 10
4.10.1.14 openSuSE Linux 10.2, 11.2
4.10.1.15 Debian GNU/Linux 3.1 r4, 5.0.3
4.10.1.16 Mandriva 2007, Corporate Server 5
4.10.1.17 Ubuntu 8.04.2 Server Edition
4.10.1.18 Ubuntu 9.10 Server Edition

4.10.2 Características:

4.10.2.1 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
4.10.2.2 Capacidade de verificar tráfego HTTP 1.0 e 1.1 (RFC 2616), FTP (RFC 959, 2389, Extensões para FTP) e FTP sobre HTTP;
4.10.2.3 Capacidade de definir listas de tipos de objetos que não serão verificados;
4.10.2.4 Capacidade de definir listas de servidores que não terão o tráfego verificado;
4.10.2.5 Capacidade de definir grupos de usuários e aplicar regras de verificação por grupos;
4.10.2.6 Capacidade de iniciar várias cópias do processo de antivírus;
4.10.2.7 Capacidade de escolher o tamanho reservado na memória para armazenamento dos arquivos que serão verificados;

4.10.3 Capacidade de escolher o tamanho do buffer do arquivo a ser verificado;

4.10.4 Capacidade de escolher o número máximo de objetos na fila de verificação;

4.10.5 Capacidade de definir o tempo máximo de verificação de um objeto;

4. DA PRESTAÇÃO DOS SERVIÇOS – INSTALAÇÃO E SUPORTE

4.1 A Contratada deverá instalar o produto em todos os equipamentos do Conselho, incluindo dispositivos móveis, estações de trabalho e servidores, a console de gerenciamento e sua configuração.

4.2. A Contratada deverá disponibilizar **serviço "ON SITE", durante 180 dias**, contados a partir do recebimento, com a finalidade de instalar, solucionar eventuais problemas, operação e configuração ou qualquer outra atividade em que qualifique o software. Para tanto é necessária a presença de um técnico da empresa contratada sempre que houver um chamado, com prazo máximo de atendimento de 6 horas na sede do CRCRS.

5. DO LOCAL E DO PRAZO DE INSTALAÇÃO E CONFIGURAÇÃO

5.1. Os serviços de instalação e configuração serão realizados na sede do CRCRS, Av,. Praia de Belas, 1554 – Menino Deus em Porto Alegre-RS.

5.2. O prazo máximo para a instalação completa de todas as unidades será de **05 (cinco) dias úteis** a partir da assinatura do contrato.

6. DA QUALIFICAÇÃO TÉCNICA

A capacidade técnica e operacional deverá ser comprovada mediante apresentação de atestados emitidos por pessoas jurídicas de direito público ou privado que tenham contratado junto a ofertante, que comprovem a execução prévia de objeto semelhante ao ora licitado. Considerando a dimensão do presente objeto, será exigido:

I – Ao menos um atestado comprovando a comercialização de lote de licenças de qualquer software.

II – Ao menos um atestado, comprovando a realização de serviço de instalação, treinamento e manutenção de solução antivírus.

7. CRITÉRIO DE JULGAMENTO DA PROPOSTA

O critério de julgamento dos preços será de "MENOR PREÇO POR LOTE".

8. DA PROPOSTA DE PREÇOS

8.1. A proposta de preços deverá discriminar:

a) O valor unitário por licença;
b) O valor dos serviços de implantação, treinamento e suporte.

8.2. O julgamento da proposta será pelo critério de MENOR VALOR GLOBAL, considerando a seguinte fórmula: VALOR GLOBAL = VALOR UNITÁRIO DA LICENÇA X 180 UNIDADES + VALOR SERVIÇO

9. DAS OBRIGAÇÕES

São obrigações da CONTRATADA, além de outras especificadas no edital, na proposta e/ou no contrato:

a) manter durante toda a execução do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

b) manter atualizado endereço, inclusive eletrônico, e telefones cadastrados junto ao CONTRATANTE para comunicações, informando imediatamente eventual alteração;

c) sempre que solicitado, apresentar, documentos que comprovem o cumprimento da legislação em vigor quanto às obrigações assumidas na licitação;

d) acatar as exigências do CRCRS quanto a normas de controle interno e rotinas de serviço;

e) comprovar, a qualquer momento, o pagamento dos tributos que incidirem sobre a execução dos serviços prestados.

10. DAS PENALIDADES

Ressalvadas as situações de caso fortuito e de força maior regularmente alegadas e provadas, a CONTRATADA sujeita-se às seguintes penalidades:

10.1. Advertência, caso ocorram pequenas irregularidades que não caracterizem descumprimento de cláusula contratual;

10.2. Multa, calculada sobre o valor total do contrato:

b) 1% (um por cento) nos casos de descumprimento de cláusula contratual que não inviabilize o cumprimento do contrato;

c) 1% (um por cento) por dia de atraso no cumprimento de prazos;

d) em caso de rescisão do contrato por ato ou omissão da CONTRATADA, 20% (vinte por cento) sobre o valor da parcela não adimplida;

10.3 Suspensão do direito de licitar e contratar com o CONTRATANTE, pelo prazo de até 2 (dois) anos.

10.4. Declaração, pelo Presidente do CONTRATANTE, da inidoneidade da CONTRATADA.

Parágrafo primeiro: A aplicação de uma das penalidades previstas nesta Cláusula, não elide a aplicação das demais, podendo haver aplicação concomitante.

Parágrafo segundo. A aplicação de penalidade não será efetuada sem notificação prévia da CONTRATADA.

Parágrafo terceiro. O valor da(s) multa(s) será descontado de eventuais pagamentos devidos à CONTRATADA, ou, cobrado diretamente, caso inexistam valores a serem pagos ou o valor da multa seja superior a estes.

Parágrafo quarto. A penalidade prevista no item 10.3 poderá ser aplicada caso a CONTRATADA demonstre conduta eivada de má-fé, ou, de qualquer forma incompatível com a seriedade do procedimento, como tais consideradas o retardamento injustificado do cumprimento do objeto do presente contrato, a recusa injustificada de assinatura do contrato, a não manutenção da proposta de modo injustificado, a perda das condições de

habilitação não informada imediatamente ao CONTRATANTE, o cometimento de fraudes e o comportamento inidôneo.

Parágrafo quinto. A penalidade prevista no item 10.4 será aplicável em caso de reiteração de condutas previstas no parágrafo anterior, ainda que não tenha sido aplicada a penalidade prevista, bem como, no de comprovado envolvimento em ilícitos penais ou fiscais.
Parágrafo sexto. As penalidades aqui cominadas são de caráter administrativo, e não limitam a atuação do CRCRS na esfera cível para ressarcimento de dano, inclusive moral.

11. DA VIGÊNCIA

11.1. O contrato vigerá pelo prazo de 12 (doze) meses, prorrogável até o limite de 48 (quarenta e oito) meses, por conveniência do CRCRS.

11.2. Por ocasião da renovação, o valor contratual poderá ser reajustado por índices oficiais.

12. DO VALOR DE REFERÊNCIA

O valor referencial não será divulgado, vez que a publicação é mera faculdade da Administração, que pode utilizar a omissão como estratégia para busca do menor preço, prática respaldada pelo Tribunal de Contas da União, como se extrai de seu Informativo de Licitações e Contratos nº 51:

> *No caso do pregão, a divulgação do valor orçado e, se for o caso, do preço máximo, caso este tenha sido fixado, é meramente facultativa*
> *Na mesma representação pela qual o Tribunal tomou conhecimento de potenciais irregularidades no Pregão nº 208/2010, realizado pelo Ministério da Saúde - MS, analisou-se, como possível irregularidade, a não divulgação dos valores de referência, tidos, na espécie, como preços máximos a serem praticados, que teria resultado em prejuízo para a elaboração da proposta por parte das empresas licitantes. Em seus argumentos, o MS defendeu tratar-se de estratégia, a fundamentar a negociação a ser travada entre pregoeiro e as licitantes. Nesse quadro, levantou precedente no qual o TCU entendeu ser facultativa a divulgação dos valores de referência. Para o órgão, "a revelação do preço máximo faz com que as propostas das licitantes orbitem em torno daquele valor, o que poderia frustrar a obtenção das melhores condições de contratação". Já para a unidade técnica, existiriam, no TCU, duas correntes acerca da necessidade da divulgação de orçamento/preço máximo em edital. Pela primeira, "no caso específico dos pregões, [...] o orçamento estimado em planilhas e os preços máximos devem necessariamente fazer parte do Termo de Referência, na fase preparatória do certame, e a sua divulgação é decisão discricionária do órgão organizador". Para a outra corrente, que "abarca as situações que não sejam de pregões, tem-se farta jurisprudência no sentido de que o disposto do art. 40, inc. X, da Lei 8.666 obriga, e não faculta, a divulgação do orçamento estimado em planilhas e de preços máximos no instrumento convocatório". Assim, para a unidade técnica, à exceção do pregão, a jurisprudência do TCU, apoiada pela doutrina, majoritariamente considera "a divulgação do 'orçamento ou preço máximo no instrumento convocatório' como elemento imperativo, e não meramente opcional". Contudo, ainda de*

> *acordo com a unidade instrutiva, o acórdão nº 3.028/2010, da 2ª Câmara, teria aberto precedente, no sentido de se interpretar "a divulgação dos preços máximos, prevista no art. 40, X, da Lei 8.666/93, como facultativa, e não obrigatória, sem ressalvas com relação à modalidade da licitação". Em razão da aparente divergência jurisprudencial, a unidade técnica sugeriu que a questão fosse apreciada em sede de incidente de uniformização de jurisprudência, com o que discordou o relator. Para ele, "o art. 40, X, da Lei nº 8.666/93 não discorre sobre a 'divulgação' do preço máximo, mas sim sobre a sua "fixação", o que é bem diferente". A fixação de preços máximos, tanto unitários quanto global, seria obrigatória, no entender do relator, no caso de obras e serviços de engenharia, nos termos da Súmula TCU nº 259/2010, donde se concluiria que, para outros objetos, não relacionados a obras e serviços de engenharia, essa fixação é meramente facultativa. Fez ressalva, todavia, ao caso do pregão, para o qual, "a jurisprudência do TCU acena no sentido de que a divulgação do valor orçado e, se for o caso, do preço máximo, caso este tenha sido fixado, é meramente facultativa". Precedente citado: Acórdão nº 3.028/2010, da 2ª Câmara. Acórdão n.º 392/2011-Plenário, TC-033.876/2010-0, rel. Min. José Jorge, 16.02.2011.*

Frise-se que a restrição à divulgação do valor referencial se estende à disponibilização de documentos específicos do processo administrativo que contenham tais informações antes da sessão pública, evitando-se fulminar a efetividade da estratégia. Ademais, ao não divulgar o valor orçado, mas possibilitar vistas dos respectivos documentos, haveria prejuízo a isonomia do certame, privilegiando-se os interessados locais. Neste sentido, o AC-2080-30/12-P do TCU:

> *VOTO*
>
> *(…)*
>
> *6. Quanto ao primeiro ponto do edital questionado pela representante, é firme o entendimento deste Tribunal no sentido de que a Administração não está obrigada a anexar ao edital o orçamento de referência da licitação, mas tão somente constar o documento do respectivo procedimento administrativo, conforme a exegese que se faz do art. 3º, inciso III, da Lei n.º 10.520/2002, nos termos da jurisprudência referenciada.*
> *7. Embora também seja posição desta Corte de que a Administração deve franquear o acesso aos licitantes do referido documento, bem explicitou a instrução que há divergências acerca do momento oportuno para tanto, ou seja, antes ou depois da fase de lances, sendo apontado, neste último caso, os benefícios para manutenção do sigilo do orçamento estimativo até essa fase.*
> *8. Conquanto a ampla publicidade seja imperativa na Administração Pública, julgo que, em situações semelhantes a que se apresenta, o acesso ao referido orçamento colidiria com outros princípios não menos importantes, como o da busca da proposta mais vantajosa para a administração, de modo que a reserva do seu conteúdo não se configura violação ao princípio da publicidade, nem*

mesmo ao seu propósito de assegurar o controle pela sociedade da legalidade e legitimidade dos atos administrativos.
9. Ademais, a prática tem se revelado, inclusive no âmbito do próprio FNDE, que a manutenção do sigilo do orçamento estimativo tem sido positiva para Administração, com a redução dos preços das contratações, já que incentiva a competitividade entre os licitantes, evitando assim que os concorrentes limitem suas ofertas aos valores previamente cotados pela Administração.
10. A propósito, lembro que o procedimento adotado pelo FNDE segue recomendação a ele dirigida por este Tribunal por meio Acórdão 1789/2009 – Plenário, que trouxe como fundamento essencial de decidir o entendimento de que o acesso ao orçamento antes da fase de lances poderia representar violação ao princípio da isonomia, nos termos do que constou do respectivo Voto condutor, conforme transcrito na instrução da unidade técnica.

13. DOS RECURSOS FINANCEIROS

Os recursos financeiros para pagamento do objeto da presente licitação correrão por conta do elemento de despesa “Aquisição de Softwares”.

14. DO PAGAMENTO

14.1. De acordo com o artigo 64 da lei n° 9.430, de 27.12.96, os pagamentos efetuados por órgãos, autarquias e fundações da administração pública federal a pessoas jurídicas, pelo fornecimento de bens ou prestação de serviços, estão sujeitos à incidência, na fonte, do imposto sobre a renda, da contribuição social sobre o lucro líquido, da contribuição para seguridade social – Cofins e da Contribuição para o Pis/Pasep.

14.2. A tabela de bens e serviços a que se refere o item anterior está à disposição de todos os interessados no site da Receita Federal www.receita.fazenda.gov.br, (INs SRF nº 1234/12 e alterações).

14.3. Após a apresentação e verificação da regularidade da nota fiscal, o pagamento será efetuado em até 10 (dez) dias úteis.

15. DA FISCALIZAÇÃO

15.1. A fiscalização será exercida no interesse do CRCRS e não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por quaisquer irregularidades e, na sua ocorrência, não implica corresponsabilidade do CRCRS ou de seus agentes e prepostos.

15.2. As decisões e providências que ultrapassarem a competência do fiscal designado deverão ser solicitadas ao seu gestor, em tempo hábil para adoção das medidas convenientes.

15.3. A CONTRATADA deverá indicar um preposto para representá-la junto ao fiscal do contrato.

16. DISPOSIÇÕES GERAIS

17.1. As notificações poderão ser formalizadas por meio eletrônico.

17.2. É vedada a subcontratação, salvo com anuência expressa do CONTRATANTE e desde que a subcontratada comprove preencher todos os requisitos de habilitação para contratação com o Poder Público.

PREGÃO ELETRÔNICO CRCRS 15/2016

PROCESSO ADMINISTRATIVO 104/2016

ANEXO II

MINUTA DE CONTRATO

Pelo presente instrumento particular, de um lado, o **CONSELHO REGIONAL DE CONTABILIDADE DO RIO GRANDE DO SUL**, entidade de fiscalização do exercício da profissão contábil, com sede nesta Capital, na Avenida Praia de Belas 1.554, inscrita no CNPJ sob o nº 92.698.471/0001-33, neste ato representada por seu Presidente, Contador Antônio Carlos de Castro Palácios, doravante denominado **CONTRATANTE**, e, de outro lado, **XXXXXXXXXXXXX**, inscrita no CNPJ sob nº XXXXXXXX, com sede XXXXXXXXXXXXX, doravante denominada **CONTRATADA**, celebram o presente contrato que decorre e tem seu fundamento no processo administrativo CRCRS **nº 104-16** e se rege pelo disposto na Lei 8.666/93, pelo edital, pela proposta e demais elementos do referido processo, os quais consideram-se parte integrante e complementar do presente contrato, bem como, nas cláusulas e condições a seguir especificadas:

CLÁUSULA PRIMEIRA- DO OBJETO:

O objeto da presente Licitação é a aquisição de licenças de Software Antivírus com fornecimento de 180 licenças para estações de trabalho, dispositivos móveis e servidores, incluindo instalação, configuração e serviço de suporte “ON SITE” durante os primeiros 180 dias, contados da implementação, contemplando atualizações do banco de dados de ameaças, por um período de 3 anos, conforme especificações do Anexo I do Edital 15/2016.

CLÁUSULA SEGUNDA - DA PRESTAÇÃO DOS SERVIÇOS – INSTALAÇÃO E SUPORTE

2.1 A Contratada deverá instalar o produto em todos os equipamentos do conselho, incluindo dispositivos móveis, estações de trabalho e servidores, a console de gerenciamento e sua configuração.

2.2. A Contratada deverá disponibilizar serviço “ON SITE”, durante 180 dias, contados a partir do recebimento, com a finalidade de instalar, solucionar eventuais problemas, operação e configuração ou qualquer outra atividade em que qualifique o software. Para tanto é necessária a presença de um técnico da empresa contratada sempre que houver um chamado, com prazo máximo de atendimento de 6 horas na sede do CRCRS.

CLÁUSULA TERCEIRA –DO LOCAL E DO PRAZO DE INSTALAÇÃO E CONFIGURAÇÃO

3.1. Os serviços de instalação e configuração serão realizados na sede do CRCRS, Av,. Praia de Belas, 1554 – Menino Deus em Porto Alegre-RS.

3.2. O prazo máximo para a instalação completa de todas as unidades será de 05 (cinco) dias úteis a partir da assinatura do contrato.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES

São obrigações da CONTRATADA, além de outras especificadas no edital, na proposta e/ou no contrato:

a) manter durante toda a execução do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

b) manter atualizado endereço, inclusive eletrônico, e telefones cadastrados junto ao CONTRATANTE para comunicações, informando imediatamente eventual alteração;

c) sempre que solicitado, apresentar, documentos que comprovem o cumprimento da legislação em vigor quanto às obrigações assumidas na licitação;

d) acatar as exigências do CRCRS quanto a normas de controle interno e rotinas de serviço;

e) comprovar, a qualquer momento, o pagamento dos tributos que incidirem sobre a execução dos serviços prestados.

CLÁUSULA QUINTA - DAS PENALIDADES

Ressalvadas as situações de caso fortuito e de força maior regularmente alegadas e provadas, a CONTRATADA sujeita-se às seguintes penalidades:

5.1. Advertência, caso ocorram pequenas irregularidades que não caracterizem descumprimento de cláusula contratual;

5.2. Multa, calculada sobre o valor total do contrato:

b) 1% (um por cento) nos casos de descumprimento de cláusula contratual que não inviabilize o cumprimento do contrato;

c) 1% (um por cento) por dia de atraso no cumprimento de prazos;

d) em caso de rescisão do contrato por ato ou omissão da CONTRATADA, 20% (vinte por cento) sobre o valor da parcela não adimplida;

5.3 Suspensão do direito de licitar e contratar com o CONTRATANTE, pelo prazo de até 2 (dois) anos.

5.4. Declaração, pelo Presidente do CONTRATANTE, da inidoneidade da CONTRATADA.

Parágrafo primeiro: A aplicação de uma das penalidades previstas nesta Cláusula, não elide a aplicação das demais, podendo haver aplicação concomitante.

Parágrafo segundo. A aplicação de penalidade não será efetuada sem notificação prévia da CONTRATADA.

Parágrafo terceiro. O valor da(s) multa(s) será descontado de eventuais pagamentos devidos à CONTRATADA, ou, cobrado diretamente, caso inexistam valores a serem pagos ou o valor da multa seja superior a estes.

Parágrafo quarto. A penalidade prevista no item 5.3 poderá ser aplicada caso a CONTRATADA demonstre conduta eivada de má-fé, ou, de qualquer forma incompatível com a seriedade do procedimento, como tais consideradas o retardamento injustificado do cumprimento do objeto do presente contrato, a recusa injustificada de assinatura do contrato, a não manutenção da proposta de modo injustificado, a perda das condições de habilitação não informada imediatamente ao CONTRATANTE, o cometimento de fraudes e o comportamento inidôneo.

Parágrafo quinto. A penalidade prevista no item 5.4 será aplicável em caso de reiteração de condutas previstas no parágrafo anterior, ainda que não tenha sido aplicada a penalidade prevista, bem como, no de comprovado envolvimento em ilícitos penais ou fiscais.

Parágrafo sexto. As penalidades aqui cominadas são de caráter administrativo, e não limitam a atuação do CRCRS na esfera cível para ressarcimento de dano, inclusive moral.

CLÁUSULA SEXTA - DA FISCALIZAÇÃO

6.1. A fiscalização será exercida no interesse do CRCRS e não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por quaisquer irregularidades e, na sua ocorrência, não implica corresponsabilidade do CRCRS ou de seus agentes e prepostos.

6.2. As decisões e providências que ultrapassarem a competência do fiscal designado deverão ser solicitadas ao seu gestor, em tempo hábil para adoção das medidas convenientes.

6.3. A CONTRATADA deverá indicar um preposto para representá-la junto ao fiscal do contrato.

CLÁUSULA SÉTIMA – DO PREÇO:

7.1. O valor referente unitário por licença será de R$ XX,XX, perfazendo um total de R$ XX,XX

7.2. O valor referente ao serviço de instalação, configuração e suporte será de R$ XX,XX.

7.3. O valor global do contrato será a soma dos itens acima, perfazendo um total de R$ XX,XX

7.4. No valor estão inclusos eventuais descontos e/ou vantagens adicionais, assim como todas as despesas relativas ao objeto do presente contrato, inclusive impostos federais, estaduais e/ou municipais porventura incidentes, seguros, taxas e/ou emolumentos, mão-de-

obra, materiais, equipamentos, ferramentas, amostras e quaisquer outras não expressas no presente contrato.

CLÁUSULA OITAVA – DOS RECURSOS FINANCEIROS:

Os recursos financeiros para pagamento do objeto da presente licitação correrão por conta dos elementos de despesa “Aquisição de Software”.

CLÁUSULA NONA – DO PAGAMENTO:

9.1. De acordo com o artigo 64 da lei n° 9.430, de 27.12.96, os pagamentos efetuados por órgãos, autarquias e fundações da administração pública federal a pessoas jurídicas, pelo fornecimento de bens ou prestação de serviços, estão sujeitos à incidência, na fonte, do imposto sobre a renda, da contribuição social sobre o lucro líquido, da contribuição para seguridade social – Cofins e da Contribuição para o Pis/Pasep.

9.2. A tabela de bens e serviços a que se refere o item anterior está à disposição de todos os interessados no site da Receita Federal www.receita.fazenda.gov.br, (INs SRF nº 1234/12 e alterações).

9.3. Após a instalação e configuração, e apresentada e verificada a regularidade da nota fiscal, o pagamento será efetuado em até 10 (dez) dias úteis.

CLÁUSULA DÉCIMA - DA VIGÊNCIA

10.1. O contrato vigerá pelo prazo de 12 (doze) meses, prorrogável até o limite de 48 (quarenta e oito) meses, por conveniência do CRCRS.

10.2. Por ocasião da renovação, o valor contratual poderá ser reajustado por índices oficiais.

CLAÚSULA DÉCIMA-PRIMEIRA – DA RESCISÃO:

O presente contrato poderá ser rescindido a qualquer tempo:

a) por ato unilateral e escrito do CONTRATANTE nos casos previstos nos incisos I a XII e XVII do artigo 78 da Lei 8.666/93;
b) por acordo entre as partes, reduzido a termo, desde que haja conveniência para o CONTRATANTE.
c) judicialmente, nos termos legais.

Parágrafo primeiro. Independentemente da aplicação das penalidades previstas no presente contrato, nos casos de rescisão em virtude de inadimplemento contratual, a parte inadimplente ressarcirá à outra por todos os prejuízos decorrentes da rescisão.

Parágrafo segundo. A CONTRATADA reconhece os direitos do CONTRATANTE em caso de rescisão administrativa prevista no artigo 77 da Lei 8.666/93.

CLÁUSULA DÉCIMA-SEGUNDA - DO FORO:

Fica eleita a Justiça Federal, Subseção Judiciária de Porto Alegre, como foro para dirimir eventuais litígios oriundos do presente contrato, com renúncia de qualquer outro, ainda que mais privilegiado.

CLÁUSULA DÉCIMA-TERCEIRA – DAS DISPOSIÇÕES GERAIS:

15.1. As notificações poderão ser formalizadas por meio eletrônico.

15.2. A tolerância das partes relativamente a infrações às disposições constantes do presente instrumento, não exime o infrator de cumprir com todas as obrigações assumidas, podendo ser-lhe exigida, a qualquer tempo, o cumprimento integral.

15.3. Aumento e diminuição do objeto observarão os limites legais e o incremento ou decréscimo ocorrerá de forma proporcional ao preço licitado.

Por estarem em acordo com os termos do presente instrumento, após a leitura do mesmo, firmam-no as partes em 2 (duas) vias de igual teor e forma, junto a duas testemunhas que também subscrevem.

Porto Alegre, xx de XXXX de 2016.

CRCRS

Contratada

Testemunhas - _____ _____