TERMO DE CONTRATO Nº 10 /2018

Pelo presente instrumento contratual, de um lado a **FARMÁCIA DO IPAM LTDA**., com sede na Rua Pinheiro Machado, nº 2281, Centro, CEP 95020-172, fone: (54) 4009-7700, nesta cidade de Caxias do Sul – RS, inscrita no CNPJ sob o número 88.635.305/0001-10, adiante denominada simplesmente **CONTRATANTE**, neste ato representado por Diretora Sra. CLAUDETE KREMER SOTT, CPF n° 596.833.920-91, residente e domiciliada nesta cidade, e, de outro lado, a empresa **INTRODUCE LTDA**, com sede na Av. Therezinha Pauletti Sanvitto, n°208, sala, 809, Bairro Sanvitto, CEP 95110-195, fone: (54) 3041-5254, na cidade de Caxias do Sul/RS, inscrita no CNPJ n° 18.945.982/0001-50, representada por seu Representante Legal, Sr. MAURICIO GIMENES DA SILVA portador do CPF n°025.779.060-80, residente e domiciliado na cidade de Caxias do Sul, adiante denominada simplesmente **CONTRATADA**, mediante as cláusulas seguintes, convencionam:

CLÁUSULA PRIMEIRA: DA BASE LEGAL.

Aplicam-se ao presente contrato as disposições da Lei 13.303/2016, diante do contido no **Processo Administrativo nº 21/2018**, que trata de Dispensa de Licitação, nos termos do **artigo 29, inciso II** da Lei 13.303/2016, e sujeitando-se à Lei 5.285 de 29 de Novembro de 1999, que trata do Cadastro de Fornecedores impedidos de licitar e contratar com a Administração Pública Municipal.

CLÁUSULA SEGUNDA: DO OBJETO.

2.1. O objeto contratual consiste no desenvolvimento, implementação, integração e suporte aos serviços de informática, tais como: INTERNET, FIREWALL, DHCP, PROXY, EMAIL, Servidor WEB, Servidor de Dados, Autenticação, Impressão, Backup e Antivírus, bem como o desenvolvimento de scripts para importação, exportação e transferências de arquivos entre a farmácia com o IPAM, utilizando-se de ferramenta **gerencial única** para a Farmácia do IPAM Ltda., conforme especificações constantes no **Anexo I**, parte integrante do presente contrato.

CLÁUSULA TERCEIRA: DA EXECUÇÃO DO OBJETO.

3.1. Os serviços descritos na Cláusula Segunda e Anexo I do presente contrato foram desenvolvidos e implementados de acordo com o Hardware disponibilizado pela CONTRATANTE.

> **3.1.1.** O objeto apresentado ao Anexo I trata-se de especificações técnicas, as quais suprem as necessidades da CONTRATANTE, podendo ser admitido ao longo da execução contratual, o fornecimento pela CONTRATADA, de soluções similares ou superiores às apresentadas, desde que sejam efetivados todos os pontos constantes no anexo supracitado e não gerem qualquer custo adicional à CONTRATANTE.

3.2. Os serviços contratados serão desenvolvidos nas instalações da CONTRATADA ou nas instalações da CONTRATANTE, quando a necessidade do serviço a ser executado assim o determinar, sem comprometer a exatidão e eficiência do mesmo.

3.3. Os serviços objeto do presente contrato, foram desenvolvidos e implementados pela empresa CONTRATADA e deverão estar ativos, bem como deverá ser dado suporte conforme item 3.4, a partir do dia 05 de dezembro de 2018.

3.4. O suporte técnico será realizado pela CONTRATADA, através de Central de Suporte, que será disponibilizada 24 horas por dia, 365 dias por ano.

3.4.1. O tempo máximo para retorno do atendimento será de 2 horas, a partir da abertura do chamado realizado pela CONTRATANTE, e de até 6 horas para resolução dos problemas.

3.4.2. Em caso de paralisação dos serviços, o tempo de resposta para os chamados será de 1 hora, a contar da comunicação e de até 4 horas para a resolução dos problemas.

CLÁUSULA QUARTA: DO RECEBIMENTO.

4.1. Para o recebimento dos serviços objetos deste contrato, a CONTRATANTE designará o funcionário Felipe Remi Caldart, que fará o recebimento dos serviços, observando o seguinte:

a) Provisoriamente, no ato de recebimento dos serviços (antivírus e testes do objeto contratado), para efeito de posterior verificação da conformidade com o solicitado ao Anexo I;

b) Definitivamente, com a emissão do respectivo Termo de Recebimento, após o decurso do prazo de observação dos serviços e conseqüente aceitação, no prazo máximo de **05 (cinco) dias úteis** contados após o recebimento provisório, nos termos da alínea 'a' do subitem 4.1 deste Contrato.

4.2. Quando da verificação que os serviços não atendem às especificações solicitadas, serão aplicadas as sanções previstas na **Cláusula Nona** deste contrato.

CLÁUSULA QUINTA: DAS OBRIGAÇÕES DA CONTRATADA.

5.1. Cumprir fielmente o contrato, bem como manter todas as condições de habilitação e qualificação exigidas no momento da contratação, durante toda a execução do presente contrato, em compatibilidade com as obrigações assumidas.

5.1.1. Toda e qualquer prestação de serviços em desacordo com o estabelecido neste contrato será imediatamente notificada à CONTRATADA, que ficará obrigada a refazê-los, ficando entendido que correrão

por sua conta e risco tais serviços, podendo ser aplicadas também as sanções previstas na Cláusula Nona deste contrato.

5.1.2. Deverá informar à CONTRATANTE qualquer mudança de endereço, de telefone/fax ou outros meios de contatos.

5.1.3. Colocar à disposição da CONTRATANTE pessoal apto a executar os serviços contratados, no que tange a idoneidade e competência, responsabilizando-se pelo pagamento das despesas com os mesmos.

5.1.4. Arcar com todas as obrigações previdenciárias, fiscais, comerciais, trabalhistas, tributárias, máquinas, materiais e equipamentos necessários para a prestação dos serviços, responsabilidade civil, acidentes de trabalho, pessoal capacitado e treinado para os serviços, deslocamento, alimentação, hospedagem, suporte técnico e demais despesas incidentes ou que venham a incidir sobre os serviços, objeto deste contrato.

5.1.4.1. A inadimplência da CONTRATADA com relação aos encargos sociais, trabalhistas, fiscais e comerciais ou indenizações, não transfere à CONTRATANTE a responsabilidade por seu pagamento, nem poderá onerar o objeto contratado, de acordo com o artigo artigo 77, parágrafo 1º da Lei nº 13.303/2016.

5.1.5. Indenizar terceiros e a CONTRATANTE os possíveis prejuízos ou perdas, decorrentes de dolo ou culpa, durante a execução do contrato, em conformidade com o artigo 76 da Lei n° 13.303/2016, bem como , assumir todas as responsabilidades inerentes à sua atividade como empresa prestadora de serviços, inclusive despesas decorrentes de eventuais acidentes, abrangendo danos pessoais, corporais, morais e materiais, multas e outros danos que venham a ser causados a terceiros, ficando a CONTRATANTE isenta de qualquer tipo de responsabilidade.

5.1.6. Prestar esclarecimentos quando solicitados pela CONTRATANTE, que deverão ser realizados no prazo máximo de 05 dias consecutivos a contar da solicitação, salvo prazos estabelecidos para retorno do suporte técnico, conforme item 3.4.

5.1.7. Responsabilizar-se pela garantia de sigilo de todas as informações que venha a conhecer da CONTRATANTE, em decorrência da execução dos serviços contratados.

5.1.8. A CONTRATADA deverá disponibilizar, por meios próprios, o objeto do presente contrato, não repassando para terceiros quaisquer responsabilidades sobre o funcionamento dos mesmos.

5.1.9. No ato da assinatura do presente contrato, a CONTRATADA deverá apresentar as seguintes certificações, ou superiores:

a)Técnico certificado em Linux (Linux Professional Institute Certified Level 1), tendo em vista ser o sistema operacional utilizado nos servidores da Farmácia do IPAM Ltda.

b) Técnico certificado no antivírus ofertado.
c) Técnico certificado para suporte e atualização do Appliance UTM.
d) Técnico com Certificação Microsoft MCP.
e) Declaração do fabricante do Appliance UTM, comprovando o vínculo comercial

CLÁUSULA SEXTA: DAS OBRIGAÇÕES DA CONTRATANTE.

6.1. Proporcionar todas as facilidades necessárias à boa execução dos serviços contratados e permitir o livre acesso, mediante acompanhamento de funcionário designado pela CONTRATANTE.

6.2. Receber os serviços de acordo com o descritivo na Cláusula Quarta do presente contrato.

6.2.1. Se o serviço contratado não estiver de acordo com as condições previstas no presente contrato, a CONTRATANTE rejeitá-lo-á, no todo ou em parte, notificando à CONTRATADA para sanar as falhas e/ou refazer procedimentos.

6.3. Efetuar o pagamento nas condições estabelecidas na Cláusula Sétima do presente contrato.

6.4. Acompanhar, fiscalizar, orientar e dirimir dúvidas sobre a execução do objeto contratado.

6.5. Aplicar as penalidades legais, regulamentares e contratuais.

6.6. Esclarecer dúvidas quanto à execução dos serviços à CONTRATADA.

6.7. A CONTRATANTE ficará responsável pela comunicação à CONTRATADA quando surgirem problemas com o objeto deste contrato.

6.8. Fornecer o hardware necessário para os serviços contratados, sendo de propriedade da CONTRATANTE, e ficará situado na Rua Pinheiro Machado, n° 2281, Centro, na cidade de Caxias do Sul.

CLÁUSULA SÉTIMA: DOS VALORES E DA FORMA DE PAGAMENTO.

7.1. A CONTRATANTE pagará à CONTRATADA, pela execução do objeto do presente contratual, o valor mensal de **R$ 600,00 (seiscentos reais).**

7.1.1. O pagamento será efetuado até o 5° (quinto) dia útil do mês seguinte ao da prestação dos serviços, mediante a apresentação de Nota Fiscal.

7.1.2. O pagamento da mensalidade somente iniciará a ser computado **após a data de emissão do Termo**

de Recebimento Definitivo, ou seja, após constatação de que o mesmo foi ativado e está sendo executado a contento.

7.1.3. O pagamento relativo ao período compreendido entre o início dos serviços até o final do primeiro mês, bem como no término do contrato, será proporcionalmente ao número de dias de serviços efetivamente prestados.

7.2. A CONTRATANTE pagará pelo antivírus o valor de R$ 8.397,24 (oito mil, trezentos e noventa e sete reais e vinte e quatro centavos).

7.2.1. Deverá ser fornecido licenciamento para 85 (oitenta e cinco) usuários, pelo período de 12 meses.

7.2.2. Em casos que haja rescisão contratual, por culpa ou dolo da CONTRATADA, esta obriga-se a restituir à CONTRATANTE o **valor proporcional** pago referente ao subitem 7.2, referente aos meses em que o antivírus não será utilizado, a restituição se dará no prazo máximo de 30 dias consecutivos da rescisão, sem prejuízo da aplicação das penalidades previstas na Cláusula Nona.

7.2.3. O pagamento do antivírus será realizado mediante apresentação de nota fiscal, após a sua instalação, em quatro parcelas, sendo:

7.2.3.1. Primeira parcela a ser paga em 10 dias após a instalação.

7.2.3.2. Segunda parcela a ser paga em 30 dias após a instalação.

7.2.3.3. Terceira parcela a ser paga em 45 dias após a instalação.

7.2.3.4. Quarta parcela a ser paga em 60 dias após a instalação.

7.3. As partes efetuarão o recolhimento dos tributos devidos, cada uma delas em conformidade com as suas responsabilidades definidas em lei.

7.3.1. Nas Notas Fiscais deverá ser destacado, para posterior retenção, se devido, o Imposto Sobre Serviços (ISSQN) em cumprimento ao que dispõe a Lei Complementar nº 112, de 05 de junho de 2000.

7.4.. Os valores constantes nos itens 7.1 e 7.2 são considerados justos, relativos a todo objeto do contrato conforme item 2 e Anexo I deste contrato, inclusos valores referentes ao antivírus, bem como implementação das soluções da CONTRATADA**.**

CLÁUSULA OITAVA: DA ATUALIZAÇÃO MONETÁRIA.

8.1. No caso de prorrogação do presente contrato, a correção monetária dos valores constantes nos subitens 7.1 e 7.2 se darão depois de decorridos **12 meses** da vigência deste contrato, pelo **IGP-M/FGV** (Índice Geral de Preços de Mercado da Fundação Getúlio Vargas), acumulado no período, ou por outro índice que vier a substituí-lo.

8.2. Caso a Legislação Federal determine novos parâmetros para os reajustamentos contratuais, como periodicidade inferior a um ano, o instrumento poderá ser aditado no sentido de se adequar às novas regras.

CLÁUSULA NONA: DAS PENALIDADES E DAS MULTAS.

9.1. O cumprimento das obrigações assumidas, em desacordo com o pactuado, ou o descumprimento na totalidade, poderá acarretar à CONTRATADA as penalidades abaixo descritas, de acordo com a gravidade das mesmas, sem prejuízo das demais elencadas e na forma dos artigos 82 a 84 da Lei 13.303/2016 e Lei Municipal n°5.285/99.

9.1.1. Advertência, por escrito quando a falta for de natureza leve e não causar prejuízos a Contratante.

9.1.2. Pela recusa injustificada na entrega do objeto, por parte da CONTRATADA, nos prazos previstos no presente contrato, será aplicada multa na razão de **5%** (cinco por cento) sobre o VALOR TOTAL anual do contrato, em até 05 (cinco) dias consecutivos. Após esse prazo**,** poderá, também, ser imputada a pena prevista no subitem 9.1.6.

9.1.3. Pelo atraso ou demora injustificados para entrega do objeto, além dos prazos estipulados neste Contrato, aplicação de multa na razão de **1%** (um por cento), por dia de atraso ou de demora, calculado sobre o VALOR TOTAL anual do contrato, em até 05 (cinco) dias consecutivos de atraso ou de demora. Após esse prazo**,** poderá, também, ser imputada a pena prevista no subitem 9.1.6.

9.1.4. Pela entrega do objeto em desacordo com o solicitado, aplicação de multa na razão de **3%** (três por cento), sobre o VALOR TOTAL anual do contrato por infração, com prazo de até 02 (dois) dias úteis para adequação dos mesmos. Após 02 (duas) infrações e/ou após o prazo para adequação, poderá, também, ser imputada a pena prevista no subitem 9.1.6.

9.1.5. Quando da **reincidência em imperfeição** já notificada pela CONTRATANTE, aplicação de multa na razão de **5%** (cinco por cento) sobre o VALOR TOTAL anual do contrato, por reincidência, sendo que a CONTRATADA terá um prazo de até 02 (dois) dias consecutivos para a efetiva adequação dos mesmos. Após o prazo para adequação, poderá, também, ser imputada a pena prevista no subitem 9.1.6.

9.1.6. Suspensão de 6 (seis) meses para participar em licitação e contratação com Órgãos da Administração Municipal de Caxias do Sul.

9.2. O **atraso injustificado** no pagamento acarretará à CONTRATANTE juros moratórios de **1%** (um por cento) por mês e multa moratória de **2%** (dois por cento) sobre o total do débito.

9.3. Será facultado às partes o prazo de 05 (cinco) dias úteis para a apresentação de **Defesa Prévia**, na ocorrência de quaisquer das situações acima previstas.

9.4. Nenhum pagamento será efetuado pela CONTRATANTE enquanto pendente de liquidação qualquer obrigação financeira que for imposta à CONTRATADA em virtude de penalidade ou inadimplência contratual.

CLÁUSULA DÉCIMA: DA APLICAÇÃO DAS PENALIDADES E MULTAS.

10.1. No caso de incidência de uma das situações previstas na Cláusula Nona, a CONTRATANTE notificará a CONTRATADA para, no prazo de 05 (cinco) dias úteis, apresentar Defesa Prévia.

10.2. Será considerado justificado o inadimplemento nos seguintes casos:

a) acidentes que impliquem retardamento, inexecução dos serviços e/ou prestação dos serviços contratados em desacordo sem culpa da CONTRATADA;
b) falta ou culpa da CONTRATANTE;
c) caso fortuito ou força maior, conforme art. 393 do Código Civil Brasileiro.

10.3. O valor correspondente à aplicação das penalidades pecuniárias será reembolsado, preferencialmente, mediante desconto no pagamento das faturas relativas ao mês em que ocorrer a irregularidade. Não sendo possível o abatimento no mês de competência, o mesmo poderá ocorrer nos meses subseqüentes ou através de outra forma acordada com a CONTRATANTE.

CLÁUSULA DÉCIMA-PRIMEIRA: DOS MOTIVOS DE RESCISÃO CONTRATUAL.

11.1. São motivos de **rescisão contratual**, independente de procedimento judicial:

a) A reiteração de impugnação evidenciando a incapacidade da CONTRATADA no cumprimento satisfatório do contrato.
b) A recusa injustificada de prestação do serviço contratado; o atraso injustificado na prestação do serviço; a prestação do serviço em desacordo com o contratado; bem como quaisquer das situações previstas na Cláusula Nona deste contrato.
c) Se a CONTRATADA falir, entrar em liquidação extrajudicial e insolvência civil ou dissolução.
d) Quando ocorrerem razões de interesse público justificado.
e) A qualquer tempo, por qualquer uma das partes, desde que comunicado com antecedência mínima de 30 (trinta) dias, sem que caiba direito a qualquer tipo de indenização ou reparação à CONTRATADA, não gerando ônus de qualquer espécie e a título que for entre as partes.

11.1.1. A fusão, a cisão, e/ou a incorporação da CONTRATADA por outra empresa não serão considerados

motivos de rescisão do presente contrato desde que sejam apresentados os documentos solicitados e sejam mantidas as mesmas obrigações contratuais.

11.2. A CONTRATADA poderá declarar rescindido o presente Contrato, independente de interpelação judicial quando a CONTRATANTE atrasar os pagamentos devidos por período superior a 60 (sessenta) dias, exceto nos casos de calamidade pública, grave perturbação da ordem interna ou guerra, quando será assegurado a CONTRATADA optar pela suspensão dos serviços.

11.3. A partir da data em que for caracterizada a rescisão, cessarão as obrigações contratuais de ambas as partes, ressalvadas as vencidas até aquela data.

11.4. A CONTRATADA, em caso de rescisão administrativa, reconhece todos os direitos da CONTRATANTE.

CLÁUSULA DÉCIMA-SEGUNDA: DA VIGÊNCIA CONTRATUAL.

O presente contrato entrará em vigor na data de 05 de dezembro de 2018, com publicação de sua súmula na imprensa oficial, e vigerá pelo período de **12 meses**, podendo ser prorrogado até os limites estabelecidos na Lei 13.303/2016.

CLÁUSULA DÉCIMA-TERCEIRA: DAS DISPOSIÇÕES GERAIS.

13.1. A relação entre a CONTRATADA e a CONTRATANTE está restrita às disposições do presente contrato, não se ensejando qualquer tipo de vínculo trabalhista entre os mesmos ou seus funcionários, bem como por terceiros.

13.1.1. No caso da CONTRATANTE ser incluída no pólo passivo de demanda judicial, serão retidos pela mesma, até o final da lide, valores suficientes para garantir eventual indenização.

13.2. Os casos omissos serão resolvidos de acordo com a legislação aplicável a espécie.

CLÁUSULA DÉCIMA-QUARTA: DO FORO.

As contratantes elegem o Foro da Comarca de Caxias do Sul-RS, para dirimir dúvidas porventura emergentes da presente contratação.

E, por assim estarem justas e contratadas, as partes, por seus representantes legais, assinam o presente instrumento em 02 (duas) vias de igual teor e forma para um só e jurídico efeito, perante as testemunhas abaixo assinadas.

Caxias do Sul, de de 2018.

_____ _____

CONTRATANTE **CONTRATADA**

TESTEMUNHAS:

_____ _____

NOME: NOME:

CI: CI:

ANEXO I

CONTRATO Nº 10/2018

DESCRIÇÃO DO OBJETO DO CONTRATO

DO OBJETO:

Contratação de empresa para o desenvolvimento, implementação, integração e suporte aos serviços de informática, tais como: INTERNET, FIREWALL, DHCP, PROXY, EMAIL, Servidor WEB, Servidor de Dados, Autenticação, Impressão, Backup e Antivírus, bem como o desenvolvimento de scripts para importação, exportação e transferências de arquivos entre a farmácia com o IPAM, utilizando-se de ferramenta **gerencial única** para a Farmácia do IPAM Ltda., conforme especificações abaixo descritas:

1. A Farmácia do IPAM possui uma infra-estrutura de rede, sendo administrada de forma centralizada em sua Matriz, tendo uma quantidade **de 100 usuários**.

Matriz: Rua Pinheiro Machado, n°2281, Centro.

2. Os serviços contratados deverão ser administrados através de uma **ferramenta gerencial única**, com uma mesma base de cadastro de usuários, devendo disponibilizar todos os seus recursos para matriz.

3. A implementação deste objeto, o desenvolvimento dos serviços e demais procedimentos necessários para sua instalação deverão ser propiciados pela empresa contratada, sem nenhum acréscimo de valores além daqueles mencionados em sua proposta.

4. Os serviços mínimos a serem disponibilizados por esta ferramenta devem atender a necessidade da Farmácia do IPAM, utilizando **licenciamento durante o contrato**, em numero mínimo de 100 (cem) licenças, bem como definido junto a mesma a capacidade de hardware fornecido pela contratante necessário a sua estrutura:

4.1. Appliance UTM

4.1.1. Especificação Geral:

4.1.1.1. Produto ou OEM deve ser certificada ISO 9001-2000;
4.1.1.2. OEM deve ter presença regional de vendas e de suporte
4.1.1.3. Appliance proposto deve fornecer logs e relatórios.
4.1.1.4. Solução proposta deve cumprir as normas da FCC e CE
4.1.1.5. A solução proposta deve corresponder seguintes critérios.
a)4 Número de interface 10/100/1000
b)5000 Número de nova conexões
c) 150.000 o número de conexões simultâneas
d)1000Mbps Firewall rendimento
e) 200Mbps IPS rendimento
f)110Mpbs UTM rendimento

g) Solução deve contar com arquitetura baseada em flash

4.1.1.6. A solução proposta deve ter usuário irrestrito/ Nó de licença.

4.1.1.7. A solução proposta deve funcionar como servidor proxy HTTP autônomo com Firewall integrado, AntiVirus, Anti-Spam, filtragem de conteúdo, IPS, Firewall de Aplicação Web (WAF). QoS, Descoberta de tráfego, VPN (IPSec, SSL, L2TP, PPTP e Cisco VPN).

4.1.1.8. A solução proposta deve suportar a configuração política baseada em usuários para segurança e gerenciamento de internet.

4.1.1.9. A solução proposta deve fornecer os relatórios de appliance baseados no usuário, não só baseado em endereço IP.

4.1.2. Administração, Autenticação e Configuração geral

4.1.2.1. A solução proposta deve suportar administração via comunicação seguraHTTPS, SSH e da Console.

4.1.2.2. A solução proposta deve ser capaz de exportar e importar backup de configuração, incluindo os objetos de usuário.

4.1.2.3. A solução proposta deve suportar Route (Layer 3) / modo transparente (Layer 2).

4.1.2.4 - A solução proposta deve apoiar a integração com o Windows NTLM, Active Directory, LDAP, RADIUS ou banco de dados local para autenticação do usuário.

4.1.2.5. A solução proposta deve apoiar Automatic Single SignOn (ASSO) para autenticação do usuário.

4.1.2.6. A solução proposta deve suportar a configuração de DNS dinâmico.

4.1.2.7. A solução proposta deve fornecer gráfico de utilização de banda diário, semanal, mensal ou anual para total ou individual link ISP.

4.1.2.8. A solução proposta deve suportar Parent Proxy com suporte a IP / FQDN.

4.1.2.9. A solução proposta deve suportar NTP.

4.1.2.10. A solução proposta deverá suportar a funcionalidade de unir usuário/ip/mac para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança.

4.1.2.11. A solução proposta deve ter suporte multilíngue para console de administração web.

4.1.2.12. A solução proposta deverá suportar fazer um rollback de versão.

4.1.2.13. A solução proposta deve suportar o tempo fora de sessão e tempo ocioso forçando log out dos usuários.

4.1.2.14. A solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração.

4.1.2.15. A solução proposta deve suportar instalação de LAN by-pass no caso do appliance estar configurado no modo transparente.

4.1.2.16. A solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que PPPOEtrocar.

4.1.2.17. A solução proposta deve suportar SNMP v1, v2c e v3.

4.1.3. Multiplos ISP Load Balance e Failover

4.1.3.1. A solução proposta deve suportar Load Balance e Failover para mais de 2 ISP.

4.1.3.2. A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário, aplicação.

4.1.3.3. A solução proposta deve suportar algoritmo roundrobin para Load Balance.

4.1.3.4. A solução proposta deve fornecer opção para criar condição de Failover em ICMP, TCP ou UDP para detectar falha de conexão ISP.

4.1.3.5. A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway.

4.1.3.6. A solução proposta deve ter ativo / ativo (Round Robin) e ativo / passivo de Load Balance do gateway e suporte a Failover.

4.1.4. Firewall

4.1.4.1. A solução proposta deve ser um standaloneappliance com OS integrado.

4.1.4.2. A solução proposta deve ser ICSA &Webcoast marca firewall certificado.

4.1.4.3. A solução proposta deve suportar statefulinspection com o usuário baseado one-to-one e dinâmico NAT, PAT.

4.1.4.4. A solução proposta deve suportar a identidade do usuário como critérios de Origem / Destino IP/Subnet /group, porta de destino na regra de firewall.

4.1.4.5. A solução proposta deve facilitar a aplicação de políticas unificado de ameaças como AV / AS, IPS, filtro de conteúdo, políticas de largura de banda e política de decisão de roteamento baseado em regras de firewall para facilidade de uso, também controles unificado de ameaças deve ser aplicado sobre o tráfego entre zona.

4.1.4.6. A solução proposta deve suportar a arquitetura de segurança da zona multi-usuário definido.

4.1.4.7. A solução proposta deve ter predefinido aplicação baseado na porta/assinatura e também suportar a criação de aplicativo personalizado baseado na porta/número de protocolo.

4.1.4.8. A solução proposta deve suportar ibound NAT balanceamento de carga.

4.1.4.9. A solução proposta deve suportar 802.1q suporte marcação VLAN.

4.1.4.10 A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, ISPF, BGP4.

4.1.4. 11 A solução proposta deve suportar Cisco interface de linha de comando para roteamento estático/dinâmico.

4.1.4.12. O sistema proposto deve fornecer mensagem de alerta no Dash board sempre que a senha padrão não for alterada, o acesso seguro não é permitido e módulo subscrição está expirando.

4.1.4.13. O sistema proposto deve fornecer Mac Address (Endereço físico) regra de firewall baseada em fornecer OSI Layer 2 a Camada de segurança 7.

4.1.5. IPS

4.1.5.1. A solução proposta deve ser certificado Webcoast.

4.1.5.2. A solução proposta deve ter assinatura baseada em protocolo e sistema de prevenção de intrusão baseada em anomalia.

4.1.5.3. A solução proposta deve ter +3500 assinatura de banco de dados.

4.1.5.4. A solução proposta deve apoiar a criação da assinatura IPS personalizada.

4.1.5.5. A solução proposta deve apoiar a criação de uma política múltipla IPS para a zona diferente, em vez de política geral em nível de interface.

4.1.5.6. A solução proposta deve apoiar opção de configuração para ativar/desativar categoria/ assinatura para reduzir a latência de pacotes.

4.1.5.7. A solução proposta deve dar nome de usuário junto com IP em IPS alertas e relatórios.

4.1.5.8. A solução proposta deve levar automaticamente a atualização a partir do servidor de atualização.

4.1.5.9. A solução proposta deve apoiar o bloqueio dos Anonymous Proxy HTTP aberto rodando na porta 80 ou qualquer outra porta e também deve apoiar cliente baseado em proxy aberto como o Ultrasurf .

4.1.5.10 A solução proposta deve ser capaz de detectar e bloquear P2P aplicação baseada em mensageiro instantâneo como skype e conhecido aplicativo de bate-papo como WLM, Rediffboletc

4.1.5.11 A solução proposta deve gerar os alertas para ataques.

4.1.5.12 A solução proposta deve gerar relatórios históricos com base em mais alertas, mais atacantes, principais vítimas.

4.1.6. Gateway Anti-Virus

4.1.6.1. A solução proposta deve ter uma solução integrada de anti-vírus.

4.1.6.2. A solução proposta deve ter certificação Webcoast para antivírus / anti-spyware.

4.1.6.3. A solução proposta deve funcionar como SMTP proxy não como MTA ou servidor de retransmissão.

4.1.6.4. A solução proposta deve suportar a verificação SMTP, POP3, IMAP, FTP, HTTP, FTP através de protocolos HTTP.

4.1.6.5.O banco de dados básico de assinatura de vírus da solução proposta deve incluir a lista de assinaturas e variantes completas, bem como de malware como Phishing, spyware.

4.1.6.6. A solução proposta deve ter facilidade para adicionar assinatura/disclaimer nos e-mails.

4.1.6.7. A solução proposta deve apoiar o bloqueio dos arquivos dinâmicos/executável com base na extensão do arquivo.

4.1.6.8. Para o tráfego SMTP, a solução proposta deve apoiar seguintes ações para anexos infectados, suspeitos ou protegidos.

a. Rejeitar e-mail;

b. Entregar o correio sem anexo;

c. Entregar e-mail original;

d. Notificar o administrador.

4.1.6.9. A solução proposta deve suportar muitas políticas para anti-vírus remetente/destinatário endereço de e-mail ou grupo de endereços para configuração de notificação, quarentena configuração e extensão do arquivo, em vez de definir a política única.

4.1.6.10. A solução proposta deve atualizar a assinatura do banco de dados em uma freqüência de menos de uma hora e ele também deve suportar atualização manual.

4.1.6.11. Para o tráfego POP3 e IMAP, o sistema proposto deve retirar o anexo infectado vírus e enviar notificação ao destinatário e administrador.

4.1.6.12. A solução proposta deve analisar o tráfego HTTP baseado no nome de usuário, de origem/destino endereço IP ou URL baseada em expressão regular.

4.1.6.13. A solução proposta deve fornecer a opção para ignorar a verificação de tráfego HTTP específico.

4.1.6.14. A solução proposta deve apoiar de modo real e modo de carga para verificação de vírus HTTP.

4.1.6.15. A solução proposta deve fornecer histórico de relatórios com base no nome de usuário, endereço IP do remetente, destinatário enome dos vírus.

4.1.6.16. A solução proposta deve ter taxa de detecção de vírus acima de 98%. Apresentar o documento exigido.

4.1.7. Gateway Anti Spam

4.1.7.1. A solução proposta deve ter uma solução integrada de anti-spam.

4.1.7.2. A solução proposta deve ter certificação Webcoast para Anti Spam.

4.1.7.3. A solução proposta deve ter opções políticas configuráveis para selecionar o tráfego para verificar se há spam.

4.1.7.4. A solução proposta deve suportar verificação de spam para SMTP, POP3, IMAP.

4.1.7.5. A solução proposta deve suportar banco de dados RBL para detecção de spam.

4.1.7.6. A solução proposta deve suportar opção para arquivar e-mail para manter uma cópia dos e-mails de entrada e saída para o administrador definir endereço de e-mail.

4.1.7.7. A solução proposta deve ter múltiplas politicas configuráveispara e-mail id/endereço do grupo para a definição de quarentena, ações diferentes em vez de política geral.

4.1.7.8. A solução proposta deve apoiar a detecção de spam em tempo real e também suportar a tecnologia de detecção de vírus proativa que detecta e bloqueia os novos focos imediatamente e com precisão.

4.1.7.9. Para o tráfego SMTP, o apoio solução proposta seguintes ações

a. Marcação

b.drop

c. Rejeitar

d. Alterar destinatário

e. Entregar e-mail para o destinatário

4.1.7.10. A solução proposta deve suportarIP/Endereço lista branca/lista negra.

4.1.7.11. A solução proposta deve apoiar opção para ativar/desativar a verificação antispam para o tráfego SMTP autenticado.

4.1.7.12. A solução proposta deve apoiar a detecção de spam usando a tecnologia de detecção de padrão recorrente (RPD) para identificar o spam breaks.

4.1.7.13. A solução proposta deverá suportar a funcionalidade de detecção de spam independente da linguagem.

4.1.7.14. A solução proposta deve bloquear e-mails baseados em spam com imagens exemplo.: e-mail com texto incorporado em um arquivo de imagem.

4.1.7.15. A solução proposta deve fornecer histórico de relatórios baseado no nome de usuário, endereço IP do remetente, destinatário ecategoria spam.

4.1.7.16. A solução proposta deve fornecer Anti-Spam com função MessageDigest por usuário.

4.1.7.17. A solução proposta deve poupar largura de banda através do bloqueio de 85% das mensagens de spam a nível de gateway sem ter que baixar a mensagem usando o avançado recurso de Filtragem de Reputação de IP.

4.1.8. Solução de Proxy – Filtro web

4.1.8.1. A solução proposta deve ser certificada Webcoast.

4.1.8.2. A solução proposta deve ser solução integrada com banco de dados local em vez de requisitar ao banco de dados hospedado em algum lugar na internet.

4.1.8.3. A solução proposta deve funcionar como proxy HTTP autônomo.

4.1.8.4. A solução proposta deve ter +82 categorias no banco de dados web com 40 milhões de URL.

4.1.8.5. A solução proposta deve possuir as seguintes características:

a. Deve ser capaz de bloquear URLs baseado HTTPS com a ajuda de Certificados.

b. Caso capaz de bloquear URL com base em expressão regular

c. Devem apoiar lista de exclusão com base na expressão regular

d. Deve ter suporte para bloquear qualquer carregamento de tráfego HTTP.

e. Deve ser capaz de bloquear o Google sites em cache em base da categoria.

f. Deve ser capaz de bloquear website hospedado em Akamai.

g. Deve ser capaz de identificar e bloquear as solicitações que chegam de trás servidor proxy na base do nome de usuário e endereço IP.

h. Deve ser capaz de identificar e bloquear URL pedido de tradução.

4.1.8.6. A solução proposta deve oferecer suporte a recursos de bloqueio de controle de aplicativos

4.1.8.7. Deve ser capaz de bloquear o aplicativo Bate-papo conhecido como Yahoo, MSN, AOL, Google, Rediff, Jabberetc

4.1.8.8. Devem suportar o bloqueio de transferência de arquivos da aplicação chat conhecido e protocolo FTP.

4.1.8.9. A solução proposta deve bloquear HTTP ou HTTPS baseado na solicitação de proxy anônimo disponíveis na internet.

4.1.8.10. A solução proposta deve oferecer opção de personalizar mensagem de acesso negado para cada categoria.

4.1.8.11. A solução proposta deve ser compatível com CIPA e deve ter política de acesso predefinido CIPA baseado na Internet.

4.1.8.12. A solução proposta deve ser capaz de identificar o tráfego com base em sites produtivos, neutros, não trabalho e não especificados pelo administrador.

4.1.8.13. A solução proposta deve ter categorias específicas que reduzem a produtividade dos funcionários, a largura de banda dos sites e sites maliciosos.

4.1.8.14. A solução proposta deve ser capaz de gerar relatórios com base no nome de usuário, endereço de IP, URL, grupos, categorias e tipo de categorias.

4.1.8.15. A solução proposta deverá apoiar critérios de pesquisa em relatórios para encontrar os dados relevantes.

4.1.8.16. A solução proposta deve apoiar a criação de uma política cíclica diária/semanal/mensal/anual para acesso à internet em usuários individuais/grupo de usuários.

4.1.8.17. A solução proposta deve apoiar a criação de política de tempo de acesso à Internet para usuários individuais ou grupo.

4.1.8.18. A solução proposta deve apoiar a criação de uma política de transferência de dados diária/semanal /mensal/anual para o usuário individual ou grupo.

4.1.8.19. A solução proposta deve suportar a criação de uma política de transferência de dados cíclica diária/semanal/mensal/anual para o usuário individual ou grupo.

4.1.8.20. A solução proposta deve ter gerenciamento de banda integrado.

4.1.8.21. A solução proposta deve ser capaz de definir a largura de banda garantida e burstable por usuário/IP/Aplicação em base individual ou compartilhado.

4.1.8.22. A solução proposta deve oferecer opção de configurar diferentes níveis de prioridade para aplicação crítica.

4.1.8.23. A solução proposta deve fornecer opção para definir a largura de banda diferente para programação diferente em uma única política e largura de banda deve mudar conforme cronograma onthefly.

4.1.8.24. A solução proposta deve fornecer categoria de gerenciamento de banda baseado em web e priorização.

4.1.9. VPN

4.1.9.1. A solução proposta deve ser certificada Webcoast.

4.1.9.2. A solução proposta deve ser VPNC básico de interoperabilidade e AES certificado de interoperabilidade.

4.1.9.3. A solução proposta deve suportar IPSec (Net-to-Net, Host-to-Host, o client-to-site), L2TP e conexão VPN PPTP.

4.1.9.4. A solução proposta deve apoiar DES, 3DES, AES, Twofish, Blowfish, o algoritmo de Serpentencryption.

4.1.9.5. A solução proposta deve suportar chaves pré-compartilhadas e autenticação baseada em certificado digital.

a) A solução proposta deve suportar o modo principal e modo agressivo para uma fase de negociação.

4.1.9.6. A solução proposta deve apoiar as autoridades de certificação externa.

4.1.9.7. A solução proposta deve apoiar facilidade de exportação de configuração client-to-site para a configuração VPN sem problemas em Laptop/Desktop remoto.

4.1.9.8. A solução proposta deve apoiar os clients VPN IPSec comumente disponíveis.

4.1.9.9. A solução proposta deve apoiar a autoridade local de certificados e devem suportar criar/renovar/Excluir certificado auto-assinado.

4.1.9.10. A solução proposta deve suportar failover VPN para fins de redundância, onde mais de uma conexão estão no grupo e se uma conexão cai, muda automaticamente para outra conexão para o tempo de inatividade zero.

4.1.9.11. A solução proposta deve pré carregar certificados de terceiros, incluindo a VeriSign / Entrust.net / Microsoft e fornecer facilidade de upload de qualquer outra autoridade de certificação.

4.1.9.12. A solução proposta deve suportarThreatfree túnel VPN Ipsec/L2TP/PPTP.

4.1.10. Logging e Relatórios

4.1.10.1. A solução proposta deve ter integrado nos relatórios do appliance.

4.1.10.2. A solução proposta deve apoiar mínimos de 45 modelos diferentes para visualizar os relatórios.

4.1.10.3. A solução proposta deve fornece relatórios em HTML, CSV e formato gráfico.

4.1.10.4. A solução proposta deve suportar o registro de antivírus, antispam, filtro de conteúdo, IPS, Firewall atividade no servidor syslog.

4.1.10.5. A solução proposta deve fornece relatórios detalhados de todos os arquivos enviados via protocolo HTTP ou HTTPS. O relatóro deve incluir nome de usuário/endereço IP/URL/nome/data e hora do arquivo.

4.1.10.6. A solução proposta deve fornecer relatórios de transferência de dados na base de aplicação, nome de usuário, IP address.

4.1.10.7. A solução proposta deve fornecer relatórios de conexão completos para o usuário, IP de origem, IP de destino, porta de origem, porta de destino ou protocolo.

4.1.10.8. A solução proposta deve ter facilidade de enviar relatórios sobre o endereço e-mail ou no servidor FTP.

4.1.10.9. A solução do sistema proposto fornecer aproximados 45 relatórios regulamentares de conformidade de SOX, HIPAA, PCI, FISMA e conformidade GLBA.

4.1.10.10. A solução proposta deve apoiar facilidade auditoria para rastrear todas as atividades realizadas appliance de segurança.

4.1.10.11. A solução proposta deve apoiar vários servidores syslog para log remoto.

4.1.10.12. A solução proposta deverá apresentar ter opção configurável para enviar relatórios sobre o endereço de e-mail designado.

4.1.10.13. A solução proposta deve ser capaz de fornecer relatórios detalhados sobre todos os e-mails que passam pelo firewall.

4.1.10.14. A solução proposta deve fornecer os relatórios de todas as tentativas bloqueadas feitas por usuários/IP Address.

4.1.11. WAF

4.1.11.1. A solução proposta deve possibilitar o acréscimo de servidores com as seguintes características:

a) Web Server Name;
b) Zone;
c) Web Server Hosted On (Public IP/ FQDN ou Private IP);
d)Web Server Protocol;
e)Web Server HTTP Port;
f) SSL OffLoading;
g) Domain To Protect;
h) Exceptions;

4.1.11.2. A solução proposta deve disponibilizar configurações globais;
a) Hide Server Identity
b) Enable Passive Mode
c) Enable JavaScript Processing
d) Enable Strict HTTPS
e) Send Client IP Header
f) Allow Incomplete URLs
g) Enable Case-Sensitive URL Validation
h) EnableTransformError 500

4.1.11.3. A solução proposta deve disponibilizar Urls de erros;
a) 400 Bad Request
b) 403 Forbidden
c) 405 Method Not Allowed

4.1.11.4. A solução proposta deve disponibilizar métodos de autenticação HTTP;

4.2. Integração segura de redes remotas

4.2.1 .Recursos de tunelamento e criptografia.
4.2.2. Utilização do VNC de forma segura.

4.3. Comunicador Corporativo

4.3.1. Serviço de mensagem instantânea exclusivo para usuários autorizados.
4.3.2. Gerenciamento de usuários e grupos.
4.3.3. Auditoria de conversação entre os usuários.
4.3.4. Proxy de comunicador interno (chat), Auditoria de conversações com usuários externos.

4.4. Regras de Acesso

4.4.1. Todas as políticas de acesso são gerenciadas a partir de um único local (CPD/Matriz).
4.4.2. Serviço de publicação e assinatura de regras e informações.

4.5. E-mail Corporativo

4.5.1. Integração dos usuários e senhas com os outros serviços.

4.5.2. Suporte a múltiplos domínios, apelidos de e-mail, grupos e listas de distribuição.

4.5.3. Recursos de mensagem automática e redirecionamento de mensagem.

4.5.4. Suporte a protocolos POP e IMAP.

4.5.5. Controle de cotas de espaço de caixas de correios e tamanho de e-mails.

4.5.6. Antivírus e anti-Spam eficientes, atualizados, com checagem de veracidade do remetente.

4.5.7. Sistema de colaboração com webmail, agenda corporativa, disco virtual e outros recursos.

4.5.8. Pode operar em modo relay como filtro de entrada e saída de e-mails para servidores de e-mail: Microsoft Exchange, Lótus Notes e outros.

4.5.9. Importação dos dados atuais dos usuários.

4.6. WEB Services

4.6.1. Suporte Web para aplicações, portais, intranet e sites.

4.6.2. Suporte à PHP, CGI, JSP.

4.6.3. Múltiplos sites virtuais.

4.6.4. Configuração e implementação de domínio para INTRANET e INTERNET – para disponibilização de sites da Farmácia do Ipam.

4.7. Compartilhamento de Arquivos e Pastas com Windows

4.7.1. Compartilhamento de pastas.

4.7.2. Suporte e permissões em 3 níveis: usuário, grupos e todos.

4.7.3. Suporte de compartilhamento de aplicativos MSDos.

4.7.4. Suporte e controlador de domínio de rede Windows (manter e importar cadastro de usuários atuais – desenvolver LDAP).

4.7.5. Suporte à lixeira de arquivos de rede.

4.7.6. Definição das regras baseando-se na estrutura atual e importação dos dados atuais da Farmácia do IPAM e de seus colaboradores.

4.8. Agendamento de tarefas

4.8.1. Suporte para agendar scripts ou programas para serem executados automaticamente.

4.8.2. Tarefas recorrentes por minuto, hora, dia, semana ou mês.

4.8.3. Rotinas como: backup, limpeza de logs, verificações, relatórios, atualizações do sistema coorporativo da Farmácia do Ipam e outras.

4.9. Monitoramento on-line e estatísticas dos recursos

4.9.1. Gráfico de consumo de recursos: processamento, memória, disco e tráfego de rede.

4.9.2. Monitoramento da disponibilidade do servidor e comunicação com a internet.

4.9.3. Ações pró-ativas para restabelecimento dos serviços.

4.10. Documentação e treinamento

4.10.1. Documentação do ambiente e das configurações ativas.

4.10.2. Interface totalmente Web, amigável e 100% em português.

4.10.3. Manual de Configurações dos Recursos e Funcionalidades.

4.10.4. Treinamento de gerência dos serviços ativos.

4.11. Atualização automática e suporte técnico

4.11.1. Atualização de versões e de segurança dos principais serviços.

4.11.2. Serviço de UPdate online que verifica diariamente as atualizações no repositório da ferramenta.

4.11.3. Central de suporte com **tempo máximo** para retorno de atendimento de 1 **horas** a partir da abertura do chamado e de até 4 **horas** para deixar em plenas condições de funcionamento.

4.11.4. No caso de **funcionamento paralisado**, o tempo máximo de atendimento no local será de, no máximo, 2 **hora**a contar da comunicação e de até 6 **horas** para deixar em plenas condições de funcionamento.

4.11.5. Disponibilizar um telefone para atendimento técnico **24 horas por dia, 365 dias por ano**.

4.11.6. Abertura de chamados por telefone, painel do cliente e suporte de dúvidas por e-mail.

4.11.7. Caso haja necessidade de rever os prazos mencionados nas alíneas 'c' e 'd', conforme a gravidade do problema, deverá ser requisitado por escrito e autorizado pelo Setor de Informática da Farmácia do IPAM Ltda.

4.12. Restore automático e suporte de Hardware e Software

4.12.1. Backup das configurações.

4.12.2. Restore automatizado das configurações dos serviços.

4.12.3. Recuperação dos serviços em casos de desastres.

4.12.4. Cópia em Data Base dos dados da Farmácia do Ipam (média 80 Gb), de forma mensal e imagem da máquina ativa com os serviços.

4.12.5. Produção de Script de Backup do servidor do sistema coorporativo para este equipamento que será instalado por este objeto de contrato.

4.12.6. Implementar backup físico de hardware em equipamento disponibilizado pela Farmácia do Ipam, mantendo cópia de imagem atualizada e backup descompactado dos dados, de forma semanal.

4.13. Antivírus (Servidor de administração e console administrativa), com, no mínimo, 85 (oitenta e cinco) licenças.

4.13.1. Compatibilidade:

4.13.1.1. Microsoft Windows Server 2008

4.13.1.2. Microsoft Windows Server 2008 core

4.13.1.3. Microsoft Windows Server 2008 x64 SP1

4.13.1.4. Microsoft Windows Server 2008 R2

4.13.1.5. Microsoft Windows Server 2008 R2 core

4.13.1.6. Microsoft Windows Server 2012

4.13.1.7. Microsoft Windows XP Professional SP2 ou superior

4.13.1.8. Microsoft Windows XP Professional x64

4.13.1.9. Microsoft Windows 7

4.13.1.10. Microsoft Windows 7 x64

4.13.1.11. Microsoft Windows 8

4.13.1.12. Microsoft Windows 8 x64

4.13.2. Características

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

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

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

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

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

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

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

4.13.2.8. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

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

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

4.13.2.11. 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;

4.13.2.12. 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;

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

4.13.2.14. 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;

4.13.2.15. Deve fornecer as seguintes informações dos computadores:

4.13.2.15.1. Se o antivírus está instalado;

4.13.2.15.2. Se o antivírus está iniciado;

4.13.2.15.3. Se o antivírus está atualizado;

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

4.13.2.15.5. Minutos/horas desde a última atualização de vacinas;

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

4.13.2.15.7. Versão do antivírus instalado na máquina;

4.13.2.15.8. A necessidade de reiniciar o computador para aplicar mudanças;

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

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

4.13.2.15.11. Nome do computador;

4.13.2.15.12. Domínio ou grupo de trabalho do computador;

4.13.2.15.13. Data e horário da última atualização de vacinas;

4.13.2.15.14. Sistema operacional com Service Pack;

4.13.2.15.15. Quantidade de processadores;

4.13.2.15.16. Quantidade de memória RAM;

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

4.13.2.15.18. Endereço IP;

4.13.2.15.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.

4.13.2.15.20. Atualizações do Windows Updates instaladas;

4.13.2.15.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

4.13.2.15.22. Vulnerabilidade de aplicativos instalados na máquina.

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

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

4.13.2.17.1. Mudança de gateway;

4.13.2.17.2. Mudança de subnet DNS;

4.13.2.17.3. Mudança de domínio;

4.13.2.17.4. Mudança de servidor DHCP;

4.13.2.17.5. Mudança de servidor DNS;

4.13.2.17.6. Mudança de servidor WINS;

4.13.2.17.7. Aparecimento de nova subnet;

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

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

4.13.2.20. 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 de rede;

4.13.2.21. 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.

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

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

4.13.2.24. Deve possuir compatibilidade com Cisco Network AdminissionControl (NAC);

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

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

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

4.13.2.28. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

4.13.2.29. Capacidade de reportar vulnerabilidade de softwares presentes nos computadores.

4.13.2.30. Capacidade de realizar inventário de hardware de todas as máquinas clientes.

4.13.2.31. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes.

4.13.2.32. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

4.13.3 Estações Windows

4.13.3.1. Compatibilidade:

4.13.3.1.1. Microsoft Windows XP Professional SP3

4.13.3.1.2. Microsoft Windows 7 Professional/Enterprise/Ultimate

4.13.3.1.3. Microsoft Windows 7 Professional/Enterprise/Ultimate x64

4.13.3.1.4. Microsoft Windows 8 Professional/Enterprise

4.13.3.1.5. Microsoft Windows 8 Professional/Enterprise x64

4.13.3.2 Características:

4.13.3.2.1. Deve prover as seguintes proteções:

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

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

4.13.3.2.1.3. Antivírus de Email (módulo para verificação de emails recebidos e enviados, assim como anexos);

4.13.3.2.1.4. Antivírus de mensagens instantâneas (módulo para verificação de mensagens instantâneas, como Skype, Meebo, Yahoo Messenger, Google Talk, etc.)

4.13.3.2.1.5. Firewall com IDS;

4.13.3.2.1.6. Auto proteção (contra ataques aos serviços/ processos do antivírus);

4.13.3.2.1.7. Controle de dispositivos externos;

4.13.3.2.1.8. Controle de acesso a sites por categoria;

4.13.3.2.1.9. Controle de execução de aplicativos;

4.13.3.2.1.10. Controle de vulnerabilidade do Windows e dos aplicativos instalados;

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

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

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

4.13.3.2.5. 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");

4.13.3.2.6. 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;

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

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

4.13.3.2.9. 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;

4.13.3.2.10. Capacidade de verificar somente arquivos novos e alterados;

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

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

4.13.3.2.12.1. Perguntar o que fazer, ou;

4.13.3.2.12.2. Bloquear acesso ao objeto;

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

4.13.3.2.12.2.2. Caso positivo de desinfecção:

4.13.3.2.12.2.2.1. Restaurar o objeto para uso;

4.13.3.2.12.2.3. Caso negativo de desinfecção:

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

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

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

4.13.3.2.15. Capacidade de verificar tráfego de MSN Messenger, Google Talk (Gtalk) e Yahoo! Messenger, Skype, etc, contra vírus e links phishings;

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

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

4.13.3.2.18. Capacidade de verificação de corpo e anexos de emails usando heurística;

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

4.13.3.2.19.1. Perguntar o que fazer, ou;

4.13.3.2.19.2. Bloquear o email;

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

4.13.3.2.19.2.2. Caso positivo de desinfecção:

4.13.3.2.19.2.2.1. Restaurar o email para o usuário;

4.13.3.2.19.2.3. Caso negativo de desinfecção:

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

4.13.3.2.20. No caso do email conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

4.13.3.2.21. Possibilidade de verificar somente emails recebidos ou recebidos e enviados;

4.13.3.2.22. Capacidade de filtrar anexos de email, apagando-os ou renomeado de acordo com a configuração feita pelo administrador;

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

4.13.3.2.24. Deve ter suporte total ao protocolo IPv6;

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

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

4.13.3.2.26.1. Perguntar o que fazer, ou;

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

4.13.3.2.26.3. Permitir acesso ao objeto;

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

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

4.13.3.2.27.2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação.

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

4.13.3.2.29. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequencias características de atividades perigosas. Tais registros de sequencias devem ser atualizados juntamente com as vacinas;

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

4.13.3.2.31. 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;

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

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

4.13.3.2.34. Deve possuir módulo IDS (*IntrusionDetection System)* para proteção contra *portscans* e exploração de vulnerabilidade de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;

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

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

4.13.3.2.35.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

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

4.13.3.2.36.1. Discos de armazenamento locais;

4.13.3.2.36.2. Armazenamento removível/USB;

4.13.3.2.36.3. Impressoras;

4.13.3.2.36.4. CD/DVD;

4.13.3.2.36.5. Drives de disquete;

4.13.3.2.36.6. Modems;

4.13.3.2.36.7. Dispositivo de fita;

4.13.3.2.36.8. Dispositivos multifuncionais;

4.13.3.2.36.9. Leitores de smartcard;

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

4.13.3.2.36.11. Wi-fi;

4.13.3.2.36.12. Adaptadores de rede externos;

4.13.3.2.36.13. Dispositivos MP3 ou smartphones;

4.13.3.2.36.14. Dispositivos Bluetooth;

4.13.3.2.37. Capacidade de liberar acesso a um dispositivo específico e usuário 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;

4.13.3.2.38. Capacidade de limitar a escrita e leitura de dispositivos de armazenamento externo por usuário;

4.13.3.2.39. Capacidade de limitar a escrita e leitura de dispositivos de armazenamento externo por agendamento;

4.13.3.2.40. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

4.13.3.2.41. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc.), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;

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

4.13.3.2.43. Capacidade de bloquear execução de aplicativos que está em armazenamento externo;

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

4.13.3.2.45. 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;

4.13.3.2.46. Capacidade de, caso o computadorcliente saia da rede coorporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até o controle de aplicativos, dispositivas e acesso a web.

4.13.4 Estações de trabalho Linux.

4.13.4.1. Compatibilidade:

4.13.4.1.1. Plataforma 32-bits:

4.13.4.1.1.1. Canaima 3;

4.13.4.1.1.2. Red Flag Desktop 6.0 SP2;

4.13.4.1.1.3. Red Hat Enterprise Linux 5.8 Desktop;

4.13.4.1.1.4. Red Hat Enterprise Linux 6.2 Desktop;

4.13.4.1.1.5. Fedora 16;

4.13.4.1.1.6. CentOS-6.2;

4.13.4.1.1.7. SUSE Linux Enterprise Desktop 10 SP4

4.13.4.1.1.8. SUSE Linux Enterprise Desktop 11 SP2

4.13.4.1.1.9.openSUSE Linux 12.1;

4.13.4.1.1.10.openSUSE Linux 12.2;

4.13.4.1.1.11. Debian GNU/Linux 6.0.5.

4.13.4.1.1.12. Mandriva Linux 2011;

4.13.4.1.1.13. Ubuntu10.04 LTS;

4.13.4.1.1.14. Ubuntu12.04 LTS;

4.13.4.1.2. Plataforma 64-bits:

4.13.4.1.2.1. Canaima 3;

4.13.4.1.2.2. Red Flag Desktop 6.0 SP2;

4.13.4.1.2.3. Red Hat Enterprise Linux 5.8;

4.13.4.1.2.4. Red Hat Enterprise Linux 6.2 Desktop;

4.13.4.1.2.5. Fedora 16;

4.13.4.1.2.6. CentOS-6.2;

4.13.4.1.2.7. SUSE Linux Enterprise Desktop 10 SP4;

4.13.4.1.2.8. SUSE Linux Enterprise Desktop 11 SP2;

4.13.4.1.2.9.openSUSE Linux 12.1;

4.13.4.1.2.10.openSUSE Linux 12.2;

4.13.4.1.2.11. Debian GNU/Linux 6.0.5;

4.13.4.1.2.12. Ubuntu10.04 LTS;

4.13.4.1.2.13. Ubuntu12.04 LTS.

4.13.4.2. Características:

4.13.4.2.1. Deve prover as seguintes proteções:

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

4.13.4.2.1.2. As vacinas devem ser utilizadas pelo fabricante de, no máximo, uma em uma hora;

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

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

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

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

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

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

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

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

4.13.4.2.6. Capacidade de verificar objetos usando heurística;

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

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

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

4.13.5. Servidores Windows:

4.13.5.1. Compatibilidade:

4.13.5.1.1. Microsoft Windows Small Business Server 2011 Essentials/Standard x64;

4.13.5.1.2. Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1 x86/x64;

4.13.5.1.3. Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 x86/x64;

4.13.5.1.4. Microsoft Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1;

4.13.5.1.5. Microsoft Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1;

4.13.5.1.6. Microsoft Windows Server 2012 Fundation/Essentials/Standard x64;

4.13.5.1.7. Microsoft Windows Hyper-V Server 2008 R2 SP1;

4.13.5.1.8. Microsoft Terminal baseado em Windows Server 2008;

4.13.5.1.10. Microsoft Terminal baseado em Windows Server 2008 R2;

4.13.5.1.11. Citrix Presentation Server 4.0 e 4.5;

4.13.5.1.12. Citrix XenApp 4.5, 5.0 e 6.0.

4.13.5.2. Características:

4.13.5.2.1. Deve prover as seguintes proteções:

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

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

4.13.5.2.1.3. Firewall com IDS;

4.13.5.2.1.4. Controle de Vulnerabilidade do Windows e dos aplicativos instalados.

4.13.5.2.1.5. Capacidade de escolher de quais módulos será instalados, tanto na instalação local quanto na instalação remota;

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

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

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

4.13.5.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

4.13.5.4.3. Leitura de configurações;

4.13.5.4.4. Modificação de configurações;

4.13.5.4.5. Gerenciamento de Backup e Quarentena;

4.13.5.4.6. Visualização de relatórios;

4.13.5.4.7. Gerenciamento de relatórios;

4.13.5.4.8. Gerenciamento de chaves de licença;

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

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

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

4.13.5.5.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolhe quais portas e protocolos poderão ser utilizados.

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

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

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

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

4.13.5.5.7. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tentar gravar um arquivo infectado no servidor.

4.13.5.5.8. Capacidade de criar uma lista de máquinas que nunca serão bloqueadas mesmo quando infectadas.

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

4.13.5.5.10. 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.

4.13.5.5.11. Capacidade de pausar automaticamente varreduras caso outros aplicativos necessitem de mais recursos de memória ou processamento.

4.13.5.5.12. 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.

4.13.5.5.13. Capacidade de verificar somente arquivos novos e alterados.

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

4.13.5.5.15. Capacidade de verificar objetos usando heurística.

4.13.5.5.16. Capacidade de configurar diferentes ações para diferentes ameaças.

4.13.5.5.17. Capacidade de agendar uma pausa na verificação.

4.13.5.5.18. Capacidade de agendar uma pausa na verificação.

4.13.5.5.19. Capacidade de pausar automaticamente a verificação quando umaplicativo for iniciado.

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

4.13.5.5.20.1. Perguntar o que fazer, ou;

4.13.5.5.20.2. Bloquear acesso ao objeto;

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

4.13.5.5.20.2.2. Caso positivo de desinfecção:

4.13.5.5.20.2.2.1. Restaurar o objeto para uso;

4.13.5.5.20.2.3. Caso negativo de desinfecção:

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

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

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

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

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

4.13.6 Servidores Linux:

4.13.6.1. Compatibilidade:

4.13.6.1.1. Plataforma 32-bits:

4.13.6.1.1.1. Canaima 3;

4.13.6.1.1.2. Asianux Sever 3 SP4;

4.13.6.1.1.3. Asianux Sever 4 SP1;

4.13.6.1.1.4. Red Hat Enterprise Linux 6.2 Server;

4.13.6.1.1.5. Red Hat Enterprise Linux 5.8 Server

4.13.6.1.1.6. Fedora 16;

4.13.6.1.1.7. CentOS-6.2;

4.13.6.1.1.8. SUSE Linux Enterprise Server 11 SP2;

4.13.6.1.1.9. Novell Open Enterprise Server 11;

4.13.6.1.1.10. Open SUSE Linux 12.1;

4.13.6.1.1.11. Open SUSE Linux 12.2;

4.13.6.1.1.12. Mandriva Enterprise Sever 5.2;

4.13.6.1.1.13. Ubuntu Server 10.04.2 LTS;

4.13.6.1.1.14. Ubuntu Server 12.04 LTS;

4.13.6.1.1.15. Debian GNU/Linux 6.0.5;

4.13.6.1.1.16. FreeBSD 8.3;

4.13.6.1.1.17. FreeBSD 9.

4.13.6.1.2. Plataforma 64-bits:

4.13.6.1.2.1. Canaima 3;

4.13.6.1.2.2. Asianux Sever 3 SP4;

4.13.6.1.2.3. Asianux Sever 4 SP1;

4.13.6.1.2.4. Red Hat Enterprise Linux 6.2 Server;

4.13.6.1.2.5. Red Hat Enterprise Linux 5.8 Server

4.13.6.1.2.6. Fedora 16;

4.13.6.1.2.7. CentOS-6.2;

4.13.6.1.2.8. SUSE Linux Enterprise Server 11 SP2;

4.13.6.1.2.9. Novell Open Enterprise Server 11;

4.13.6.1.2.10. Open SUSE Linux 12.1;

4.13.6.1.2.11. Open SUSE Linux 12.2;

4.13.6.1.2.12. Mandriva Enterprise Sever 5.2;

4.13.6.1.2.13. Ubuntu Server 10.04.2 LTS;

4.13.6.1.2.14. Ubuntu Server 12.04 LTS;

4.13.6.1.2.15. Debian GNU/Linux 6.0.5;

4.13.6.1.2.16. FreeBSD 8.3;

4.13.6.1.2.17. FreeBSD 9.

4.13.6.2. Características:

4.13.6.2.1. Deve prover as seguintes proteções:

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

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

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

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

4.13.6.2.2.2. Gerenciamento de backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou

remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

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

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

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

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

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

4.13.6.2.6. C**a**pacidade de verificar objetos usando heurística;

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

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

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

4.14.7 Servidores de e-mail Windows:

4.14.7.1. Compatibilidade:

4.13.7.1.1. Microsoft Small Business Server 2008 Standard;

4.13.7.1.2. Microsoft Small Business Server 2008 Premium;

4.13.7.1.3. Microsoft Essential Business Server 2008 Standard;

4.13.7.1.4. Microsoft Essential Business Server 2008 Premium;

4.13.7.1.5. Microsoft Windows Server 2008 x64 R2 Enterprise Edition;

4.13.7.1.6. Microsoft Windows Server 2008 x64 R2 Standard Edition;

4.13.7.1.7. Microsoft Windows Server 2008 x64 Enterprise Edition SP1;

4.13.7.1.8. Microsoft Windows Server 2008 x64 Enterprise Edition SP2;

4.13.7.1.9. Microsoft Windows Server 2008 x64 Standard Edition SP1;

4.13.7.1.10. Microsoft Windows Server 2008 x64 Standard Edition SP2;

4.13.7.1.11. Microsoft Exchange Server 2010;

4.13.7.1.12. Microsoft Exchange Server 2010 SP1.

4.13.7.2. Característica:

4.13.7.2.1. Deve utilizar as tecnologias VSAPI 2.0, 2.5 e 2.6;

4.13.7.2.2. Capacidade de iniciar várias cópias do processo de antivírus

4.13.7.2.3. As vacinas devem ser utilizadas pelo fabricante de, no máximo, uma em uma hora;

4.13.7.2.4. Capacidade de verificar pastas públicas, e-mails enviados, recebidos e armazenados contra vírus, spywares, adwares, worms, trojans e riskwares;

4.13.7.2.5. Capacidade de verificar pastas públicas e e-mails armazenados de forma agendada, utilizando as últimas vacinas e heurísticas;

4.13.7.2.6. O antivírus, ao encontrar um objeto infectado, deve:

4.13.7.2.6.1. Desinfetar o objeto, notificando o recipiente, destinatário e administradores, ou;

4.13.7.2.6.2. Excluir o objeto, substituindo-o por uma notificação;

4.13.7.2.6.3. Bloquear acesso ao objeto;

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

4.13.7.2.6.3.2. Caso positivo de desinfecção:

4.13.7.2.6.3.2.1. Restaurar o objeto para o uso;

4.13.7.2.6.3.3. Caso negativo de desinfecção:

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

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

4.13.7.2.8. Capacidade de enviar notificações sobre vírus detectados para o administrador, para o recipiente e remetente da mensagem infectada;

4.13.7.2.9. Capacidade para gravar *logs* de atividade de vírus nos eventos do sistema e nos *logs* internos da aplicação;

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

4.13.8 Servidores de e-mail Lotus Notes/Dominio.

4.13.8.1. Compatibilidade:

4.13.8.1.1. Novell SuSE Linux Enterprise Server 10 x32 SP2;

4.13.8.1.2. Novell SuSE Linux Enterprise Server 10 x64 SP2;

4.13.8.1.3. Red Hat Enterprise Linux 5 x32 SP3;

4.13.8.1.4. Red Hat Enterprise Linux 5 x64 SP3;

4.13.8.1.5. Lotus Notes/Dominio 6.5;

4.13.8.1.6. Lotus Notes/Dominio 7.0;

4.13.8.1.7. Lotus Notes/Dominio 8.0;

4.13.8.1.8. Lotus Notes/Dominio 8.5;

4.13.8.2. Características:

4.13.8.2.1. Capacidade de varredura de bancos de dados internos do sistema Lotus Notes/Dominio;

4.13.8.2.2. Capacidade de varredura nas replicações de outros servidores Dominio que não tenham o antivírus instalado;

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

4.13.8.2.4. Capacidade de varredura de vírus em todos os e-mails que passam pelo sistema Lotus Notes/Dominio;

4.13.8.2.5. A varredura deve envolver o texto da mensagem e os arquivos anexos;

4.13.8.2.6. Capacidade de cura de mensagens infectadas;

4.13.8.2.7. Capacidade de filtragem de arquivos pelo tipo;

4.13.8.2.8. Capacidade de criação de Quarentena para objetos suspeitos, evitando perda de dados;

4.13.8.2.9. Capacidade de notificação do destinatário, remetente e administrador sobre objetos que contenham arquivos maliciosos;

4.13.8.2.10. Capacidade de detecção de epidemias e notificação destes eventos ao administrador;

4.13.8.2.11. Capacidade de atualização via HTTP, FTP ou pastas em rede local;

4.13.8.2.12. Capacidade de configurar o tamanho máximo de um arquivo a ser verificado.

4.13.9 Servidores de e-mail Linux:

4.13.9.1. Compatibilidade:

4.13.9.1.1. Sistemas 32-bit:

4.13.9.1.1.1. RedHat Enterprise Linux Server 5.2 Server;

4.13.9.1.1.2. Fedora 9;

4.13.9.1.1.3. SUSE Linux Enterprise Server 10 SP2;

4.13.9.1.1.4.openSUSE Linux 11.0;

4.13.9.1.1.5. Debian GNU/Linux 4.0 (r4);

4.13.9.1.1.6. Mandriva Corporate Server 4.0;

4.13.9.1.1.7. Ubuntu 8.04.1 Server Edition;

4.13.9.1.1.8. FreeBSD 6.3, 7.0.

4.13.9.1.2. Sistemas 64bits:

4.13.9.1.2.1. Fedora 9;

4.13.9.1.2.2. Red Hat Enterprise Linux Server 5.2 Server;

4.13.9.1.2.3. SUSE Linux Enterprise Server 10 SP2;

4.13.9.1.2.4. openSUSE Linux 11.0;

4.13.9.1.2.5. Debian 6.0.2.

4.13.9.1.3. MTA:

4.13.9.1.3.1. Sendmail 8.12.x ou superior;

4.13.9.1.3.2. Qmail 1.03;

4.13.9.1.3.3. Postfix 2.x;

4.13.9.1.3.4. Exim 4.x.

4.13.9.2. Características:

4.13.9.2.1. Capacidade de verificar o tráfego SMTP do servidor contra malware em todos os elementos do e-mail: cabeçalho, corpo e anexo;

4.13.9.2.2. Capacidade de notificar o administrador, o remetente e o destinatário caso um arquivo malicioso seja encontrado no e-mail;

4.13.9.2.3. Capacidade de quarentenar objetos maliciosos;

4.13.9.2.4. Capacidade de salvar backups dos objetos antes de tentativa de desinfecção;

4.13.9.2.5. Capacidade de fazer varredura no sistema de arquivos do servidor;

4.13.9.2.6. Capacidade de filtrar anexos por nome ou tipo de arquivo;

4.13.9.2.7. Capacidade de criar grupos de usuários para aplicar regras de verificação de e-mails;

4.13.9.2.8. Deve permitir gerenciamento via console WEB;

4.13.9.2.9. Deve ser atualizado de maneira automática via internet ou por servidores locais, com freqüência horária.