TERMO DE REFERÊNCIA

1. DA DESCRIÇÃO DO OBJETO

1.1. Aquisição de software de proteção antivírus, com funcionalidades antispyware, de controle de dispositivos, de prevenção de intrusos (IPS) e firewall para as estações de trabalho e servidor de arquivo da CMI, incluindo instalação, atualização de software e base de assinaturas, configuração, treinamento e suporte técnico pelo período de 36 (trinta e seis) meses, conforme especificações deste Termo de Referência.

2. DO OBJETIVO

2.1- O objeto deste Termo de Referência é a aquisição de licenças para uso de software corporativo (antivírus) para equipamentos específicos da Câmara Municipal de Ibiraçu, conforme condições, especificações técnicas e quantidades constantes neste Termo.

3. JUSTIFICATIVA DA CONTRATAÇÃO E PLANEJAMENTO

3.1 - A aquisição de licenças de uso de software corporativo (antivírus) baseia-se na política de prevenção de riscos adotada pela Câmara, cuja finalidade visa monitorar e controlar o tráfego de dados que circula entre as redes internas e a Internet, garantindo, com isso, a segurança e o bom funcionamento dos computadores da rede corporativa local (Intranet) contra ameaças maliciosas de vírus que possam causar perda de arquivos e a exploração de informações sigilosas das atividades administrativas, de dados pessoais do efetivo e do legislativo.

3.2 – Atualmente, a Câmara Municipal de Ibiraçu possui em suas instalações, 07(sete) computadores de mesa tipo desktop, 01 (um) servidor DELL rack e (01) notebook. Todavia, a Câmara Municipal viu a necessidade de aquisição de mais 2 (dois) computadores de mesa para suprir as necessidades dos servidores, a serem instalados na Secretaria da Presidência e Plenário da Câmara Municipal.

3.3 – A futura aquisição se encontra em fase de planejamento desta Câmara Municipal e são necessárias para o bom andamento dos trabalhos legislativos.

4- QUANTIDADE DE LICENÇAS

4.1 – Aquisição de 11 (onze) licenças sendo: 09 (sete) estações de trabalho do tipo Desktop, 01 (um) servidor DELL rack, (01) notebook, todos de propriedade da CMI DE IBIRAÇU conectados à rede corporativa por cabo ou rede sem fios ativos de rede.

5- DO FORNECIMENTO DO PRODUTO

5.1. O fornecimento das licenças deverá ser disponibilizado via internet pela CONTRATADA informando todos os códigos e as senhas de ativação e/ou acesso necessários ao download e instalação das licenças;

5.2 - A CONTRATADA deverá fornecer documento que comprove o direito de uso das licenças por parte da Câmara Municipal de Ibiraçu, de acordo com as exigências específicas do fabricante;

5.3 - A CONTRATADA deverá atentar ao fiel cumprimento das especificações exigidas, sendo recusado item que estiver com alguma característica diferente das especificações contidas neste termo;

5.4 - Deverá ser garantido o suporte pelo fornecedor via 0800 ou via acesso remoto

6- DAS ESPECIFICAÇÕES

6.1. As especificações relacionadas a este objeto, podem ser encontradas no Anexo I do referido Termo de Referência.

7- DA GARANTIA

7.1. Todos as licenças deverão ser garantidas pelo prazo de 03 (três) anos a partir do aceite definitivo pelo CONTRATANTE, incluindo o suporte e atualizações da solução;

7.2 - A garantia on-line deverá ser realizada durante todo o período de garantia do produto;

8- DO PRAZO DE ENTREGA E CRITÉRIOS DE RECEBIMENTO

8.1. A entrega das licenças de uso deverá ser efetuada em até 15 (quinze) dias úteis a contar da data do recebimento da Autorização de Fornecimento;

8.2 - O recebimento PROVISÓRIO ocorrerá após a entrega das licenças;

8.2.1 - O recebimento provisório das licenças não implica em aceitação das mesmas;

8.3 - O recebimento DEFINITIVO ocorrerá após a implementação e validação das licenças no servidor e homologação realizada pelo Diretor Geral da Câmara Municipal de Ibiraçu, no prazo máximo de 15 (quinze) dias úteis a contar do recebimento provisório;

8.3.1 - Havendo alguma ocorrência ou outra circunstância impeditiva, o recebimento definitivo será suspenso, até que a CONTRATADA tome as medidas saneadoras necessárias;

8.4 - O recebimento definitivo não isenta a empresa de reponsabilidades futuras quanto à qualidade do produto entregue.

9- DOS PROCEDIMENTOS DE FISCALIZAÇÃO

9.1. A fiscalização do efetivo cumprimento de tudo quanto avençado no presente instrumento caberá a Diretora Geral da Câmara, Amanda Cordeiro Dias.

9.2 - A fiscalização não exclui nem reduz a responsabilidade da CONTRATADA por quaisquer irregularidades ou vícios redibitórios e, na ocorrência destes, não implica em corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos;

10- OBRIGAÇÕES DA CONTRATATANTE

10.1 Proceder à publicação resumida do instrumento de contrato e de seus aditamentos na imprensa oficial, condição indispensável para sua validade e eficácia, no prazo de até 05 (cinco) dias corridos da sua assinatura;

10.2 Exercer a fiscalização dos serviços por servidores especialmente designados;

10.3 Efetuar o pagamento nas condições e preços pactuados no Contrato;

10.4 Notificar a CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do serviço para que sejam adotadas as medidas corretivas necessárias;

10.5 Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

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

10.7 Proporcionar todas as condições para que a CONTRATADA possa desempenhar seus serviços de acordo com as determinações deste Contrato e especialmente do

Termo de Referência e seus anexos;

10.8 Zelar para que durante toda a vigência deste contrato sejam mantidas, em compatibilidade com as obrigações assumidas pela CONTRATADA, todas as condições de habilitação.

10.9 Cumprir fielmente as disposições contidas neste Termo

11- OBRIGAÇÕES DA CONTRATADA

11.1 Responsabilizar-se integralmente pelo objeto fornecido, nas quantidades e padrões estabelecidos, sendo vedada a subcontratação, vindo a responder pelos danos causados diretamente ao CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo, nos termos da legislação vigente, não excluindo ou reduzindo essa responsabilidade a fiscalização ou acompanhamento pelo CONTRATANTE, conforme previsto no art. 70 da Lei nº 8.666/1993;

11.2 Colocar à disposição do CONTRATANTE todos os meios necessários para comprovação da regularidade do fornecimento, permitindo a verificação de suas conformidades com as especificações técnicas e exigências da contratação;

11.3 Eventuais atrasos na entrega do objeto somente serão justificáveis quando decorrerem de casos fortuitos ou de força maior, conforme disposições contidas no Código Civil Brasileiro ou por fatos de responsabilidade do CONTRATANTE;

11.4 Reparar, corrigir, remover, reconstituir ou substituir às suas expensas, no total ou em parte, no prazo máximo de 05 (cinco) dias úteis, o objeto deste Contrato em que se verificarem vícios, defeitos ou incorreções resultantes do fornecimento;

11.5 Encaminhar ao CONTRATANTE as notas fiscais relativas à contratação;

11.6 Comunicar formalmente e imediatamente ao CONTRATANTE quaisquer mudanças de endereço de correspondência, e-mail ou contato telefônico;

11.7 Cumprir todas as obrigações relacionadas ao objeto contratado, nos termos e prazos estipulados, de acordo com este Instrumento contratual;

11.8 Guardar sigilo sobre dados e informações obtidos em razão da execução deste Contrato ou da relação mantida com o CONTRATANTE;

11.9 Manter, durante toda a execução do Contrato compatibilidade com as obrigações assumidas, todas as condições de habilitação exigidas no momento da contratação.

11.10 Obedecer rigorosamente todas as normas e procedimentos de segurança implementados no ambiente de TI e institucional da Câmara Municipal de Ibiraçu;

12- DAS PENALIDADES

12.1- A empresa Contratada deverá observar rigorosamente as condições estabelecidas neste Contrato e demais anexos, sujeitando-se às penalidades constantes no art. 7º da Lei n.º 10.520/2002 e nos arts. 81, 86 e 87 da Lei n.º 8.666/1993, conforme disposto abaixo:

a) multa de 1% (um por cento) por dia, limitado a 15% (quinze por cento), incidente sobre o valor da proposta apresentada, nos casos de: descumprimento do prazo estipulado no Contrato para a retirada da Ordem de Fornecimento/Execução do Serviços; atraso quanto ao prazo de entrega dos serviços ou pela recusa em fornecer os serviços objeto deste Termo, calculada pela fórmula M = 0,01 x C x D. Tendo como correspondente: M = valor da multa, C = valor da obrigação e D = número de dias em atraso;

b) impedimento do direito de licitar e contratar com a Câmara Municipal de Ibiraçu por um período de até 2 (dois) anos, no caso de apresentação de declaração ou documento falso;

12.2 - As sanções administrativas somente serão aplicadas pela Câmara Municipal de Ibiraçu após a devida notificação e o transcurso do prazo estabelecido para a defesa prévia.

12.3 - A notificação deverá ocorrer pessoalmente ou por correspondência com aviso de recebimento, onde será indicada a conduta considerada irregular, a motivação e a espécie de sanção administrativa que se pretende aplicar, o prazo e o local de entrega das razões de defesa.

12.4 - O prazo para apresentação de defesa prévia será de 05 (cinco) dias úteis a contar da intimação, onde deverá ser observada a regra de contagem de prazo estabelecida no art. 110 da Lei n.º 8.666/1993.

13- DA RESCISÃO

13.1 - O não cumprimento das obrigações assumidas no presente contrato ou a ocorrência da hipótese prevista nos artigos 77 e 78, da Lei Federal nº 8.666, de 21 de junho de 1993, atualizada pela lei federal nº 8.883, de 8 de junho de 1994, autoriza, desde já, o CONTRATANTE a rescindir unilateralmente este contrato, independentemente de

interpelação judicial, sendo aplicável, ainda, o disposto nos artigos 79 e 80 do mesmo diploma legal, no caso de inadimplência.

13.2 - A CONTRATADA se sujeita à sanção prevista no artigo 7º da Lei Federal nº 10.520, de 17 de julho de 2002 e na Resolução nº 5, de 1º de setembro de 1993 (alterada pela Resolução nº 3/08), do CONTRATANTE, que faz parte integrante do presente ajuste.

13.3 - No caso de rescisão administrativa unilateral, a CONTRATADA reconhece o direito do CONTRATANTE de aplicar as sanções previstas no Edital, neste ajuste e na legislação que rege a licitação.

13.4- A aplicação de quaisquer sanções referidas neste dispositivo, não afasta a responsabilização civil da CONTRATADA pela inexecução total ou parcial do objeto ou pela inadimplência.

13.5- A aplicação das penalidades não impede o CONTRATANTE de exigir o ressarcimento dos prejuízos efetivados decorrentes de quaisquer faltas cometidas pela CONTRATADA.

14- DA FORMA DE PAGAMENTO

14.1- O pagamento será feito em favor da empresa Contratada, por meio de Depósito Bancário em conta corrente por ela indicada, uma vez satisfeitas as condições estabelecidas para a contratação, até o 15º (décimo quinto) dia útil após a apresentação da NOTA FISCAL devidamente discriminada e dos documentos de regularidade fiscal exigidos pelo edital, desde que não haja fato impeditivo para o pagamento.

14.3 - A nota fiscal deverá conter o mesmo CNPJ e razão social apresentados nos documentos de habilitação.

14.4 - Qualquer alteração feita no contrato social, ato constitutivo ou estatuto que modifique as informações registradas neste termo, deverá ser comunicada à Câmara Municipal de Ibiraçu, mediante documentação própria, para apreciação da autoridade competente.

14.5 - Ocorrendo erros na apresentação dos documentos fiscais, os mesmos serão devolvidos à Contratada para correção, ficando estabelecido que o prazo para pagamento será contado a partir da data de apresentação da nova fatura, devidamente corrigida sem qualquer ônus ou correção a ser paga pela Contratante.

14.6 – A Câmara Municipal de Ibiraçu poderá deduzir dos pagamentos importâncias que a qualquer título lhe forem devidas pela Contratada, em decorrência de inadimplemento contratual.

14.7 - O pagamento será feito em favor da empresa Contratada, por meio de Depósito Bancário em conta corrente por ela indicada, uma vez satisfeitas as condições estabelecidas para a contratação, desde que não haja fato impeditivo para o pagamento.

14.8 - Para a efetivação do pagamento a licitante deverá manter as mesmas condições previstas neste termo no que concerne à proposta de preço e a habilitação.

15- DA DOTAÇÃO ORÇAMENTÁRIA

15.1 - As despesas com o pagamento devido à Contratada correrão por conta da seguinte dotação constante do Orçamento para o exercício de 2021: 001001.0103100012.001 – Manutenção das atividades administrativas e legislativas da Câmara Municipal - 33904000000 – Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica.

16- VIGÊNCIA E PRORROGAÇÃO

16.1. A contratação é celebrada com vigência até ***31/12/2021****, com início a partir da publicação do extrato do contrato na Imprensa Oficial, conforme dispõe os termos do parágrafo único do art. 61, da Lei n.º 8.666/93. Expirado o prazo de vigência do contrato, subsistirá a responsabilidade da CONTRATADA sobre o tempo de validade especificado para o tipo de licença.*

17- IMPACTOS AMBIENTAIS

17.1. Não há impactos ambientais.

18-RESPONSÁVEL PELO TERMO:

Câmara Municipal de Ibiraçu. Servidor Responsável: Isabella Gomes Bottan Lombardi.

ANEXO I DO TERMO DE REFERÊNCIA

DAS ESPECIFICAÇÕES

1.1. Servidor de Administração, Console Administrativa e Compatibilidade:

1.1.1. Microsoft Windows Server 2003 SP2 (Todas edições);

1.1.2. Microsoft Windows Server 2003 x64 SP2 (Todas edições);

1.1.3. Microsoft Windows Server 2008 (Todas edições);

1.1.4.Microsoft Windows Server 2008 x64 SP1 (Todas edições);

1.1.5.Microsoft Windows Server 2008 R2 (Todas edições);

1.1.6.Microsoft Windows Server 2012 (Todas edições);

1.1.7.Microsoft Windows Server 2012 R2 (Todas edições);

1.1.8.Microsoft Windows Small Business Server 2003 SP2 (Todas edições);

1.1.9.Microsoft Windows Small Business Server 2008 (Todas edições);

1.1.10. Microsoft Windows Small Business Server 2011 (Todas edições);

1.1.11. Microsoft Windows XP Professional SP2 ou superior;

1.1.12. Microsoft Windows XP Professional x64 SP2 ou superior;

1.1.13. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;

1.1.14. Microsoft Windows VistaBusiness / Enterprise / Ultimate SP1 x64 ou posterior;

1.1.15. Microsoft Windows 7 Professional / Enterprise / Ultimate;

1.1.16. Microsoft Windows 7 Professional / Enterprise / Ultimate x64;

1.1.17. Microsoft Windows 8 Professional / Enterprise;

1.1.18. Microsoft Windows 8 Professional / Enterprise x64;

1.1.19. Microsoft Windows 8.1 Professional / Enterprise;

1.1.20. Microsoft Windows 8.1 Professional / Enterprise x64.

1.2. Suporta as seguintes plataformas virtuais:

1.2.1. VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5, ESXi 6.0;

1.2.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;

1.2.3. KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS;

1.2.4. Microsoft VirtualPC 6.0.156.0;

1.2.5. Parallels Desktop 7 e superior;

1.2.6. Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);

1.2.7. Citrix XenServer 6.1, 6.2.

1.3. Características:

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

1.3.2. Console deve ser baseada no modelo cliente/servidor;
1.3.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
1.3.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
1.3.5. 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;
1.3.6. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
1.3.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
1.3.8. 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;
1.3.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
1.3.10. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
1.3.11. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
1.3.12. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;
1.3.13. Capacidade de instalar remotamente qualquer "app" em smartphones e tablets de sistema iOS;
1.3.14. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
1.3.15. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
1.3.16. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
1.3.17. Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;
1.3.18. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
1.3.19. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

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

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

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

1.3.23. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

- *Nome do computador;*
- *Nome do domínio;*
- *Range de IP;*
- *Sistema Operacional;*
- *Máquina virtual.*

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

1.3.25. 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;

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

1.3.27. 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;

1.3.28. 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;

1.3.29. 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;

1.3.30. 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;

1.3.31. Deve fornecer as seguintes informações dos computadores:

1.3.31.1. Se o antivírus está instalado;

1.3.31.2. Se o antivírus está iniciado;

1.3.31.3. Se o antivírus está atualizado;

1.3.31.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
1.3.31.5. Minutos/horas desde a última atualização de vacinas;
1.3.31.6. Data e horário da última verificação executada na máquina;
1.3.31.7. Versão do antivírus instalado na máquina;
1.3.31.8. Se é necessário reiniciar o computador para aplicar mudanças;
1.3.31.9. Data e horário de quando a máquina foi ligada;
1.3.31.10. Quantidade de vírus encontrados (contador) na máquina;
1.3.31.11. Nome do computador;
1.3.31.12. Domínio ou grupo de trabalho do computador;
1.3.31.13. Data e horário da última atualização de vacinas;
1.3.31.14. Sistema operacional com Service Pack;
1.3.31.15. Quantidade de processadores;
1.3.31.16. Quantidade de memória RAM;
1.3.31.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
1.3.31.18. Endereço IP;
1.3.31.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
1.3.31.20. Atualizações do Windows Updates instaladas;
1.3.31.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
1.3.31.22. Vulnerabilidades de aplicativos instalados na máquina;
1.3.32. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
1.3.33. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
1.3.33.1. Alteração de Gateway Padrão;
1.3.33.2. Alteração de subrede;
1.3.33.3. Alteração de domínio;
1.3.33.4. Alteração de servidor DHCP;
1.3.33.5. Alteração de servidor DNS;
1.3.33.6. Alteração de servidor WINS;
1.3.33.7. Alteração de subrede;
1.3.33.8. Resolução de Nome;
1.3.33.9. Disponibilidade de endereço de conexão SSL;
1.3.34. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

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

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

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

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

1.3.39. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

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

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

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

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

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

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

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

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

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

1.3.49. 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.

1.3.50. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

1.3.51. Capacidade de diferenciar máquinas virtuais de máquinas físicas;

1.3.52. Gerenciamento Cifrado e Gerenciamento de Sistemas.

2. Estações Windows

2.1. Compatibilidade:

2.1.1. Microsoft Windows Embedded 8.0 Standard x64;

2.1.2. Microsoft Windows Embedded 8.1 Industry Pro x64;

2.1.3. Microsoft Windows Embedded Standard 7* x86 / x64 SP1;

2.1.4. Microsoft Windows Embedded POSReady 7* x86 / x64;

2.1.5. Microsoft Windows XP Professional x86 SP3 e superior;

2.1.6. Microsoft Windows Vista x86 / x64SP2 e posterior;

2.1.7. Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;

2.1.8. Microsoft Windows 8 Professional/Enterprise x86 / x64;

2.1.9. Microsoft Windows 8.1 Pro / Enterprise x86 / x64;

2.1.10. Microsoft Windows 10 Pro / Enterprise x86 / x64.

2.2. Características:

2.2.1. Deve prover as seguintes proteções:

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

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

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

2.2.1.4. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc);

2.2.1.5. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

2.2.1.6. Firewall com IDS;

2.2.1.7. Autoproteção (contra-ataques aos serviços/processos do antivírus);

2.2.1.8. Controle de dispositivos externos;

2.2.1.9. Controle de acesso a sites por categoria;

2.2.1.10. Controle de acesso a sites por horário;

2.2.1.11. Controle de acesso a sites por usuários;

2.2.1.12. Controle de execução de aplicativos;

2.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

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

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

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

2.2.5. 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") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.2.6. 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;

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

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

2.2.9. 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 tomar a partir da extensão do arquivo;

2.2.10. Capacidade de verificar somente arquivos novos e alterados;

2.2.11. Capacidade de verificar objetos usando heurística;

2.2.12. Capacidade de agendar uma pausa na verificação;

2.2.13. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

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

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

2.2.15.1. Perguntar o que fazer, ou;

2.2.15.2. Bloquear acesso ao objeto;

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

2.2.15.2.2. Caso positivo de desinfecção:

2.2.15.2.2.1. Restaurar o objeto para uso;

2.2.15.2.3. Caso negativo de desinfecção:

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

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

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

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

2.2.19. Capacidade de verificar links inseridos em e-mails contra phishings;

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

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

2.2.22.

2.2.23. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

2.2.23.1. Perguntar o que fazer, ou;

2.2.23.2. Bloquear o e-mail;

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

2.2.23.2.2. Caso positivo de desinfecção:

2.2.23.2.2.1. Restaurar o e-mail para o usuário;

2.2.23.2.3. Caso negativo de desinfecção:

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

2.2.24. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;

2.2.25. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

2.2.26. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

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

2.2.28. Deve ter suporte total ao protocolo IPv6;

2.2.29. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

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

2.2.30.1. Perguntar o que fazer, ou;

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

2.2.30.3. Permitir acesso ao objeto;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2.40.1. *Discos de armazenamento locais;*

2.2.40.2. *Armazenamento removível;*

2.2.40.3. *Impressoras;*

2.2.40.4. *CD/DVD;*

2.2.40.5. *Drives de disquete;*

2.2.40.6. *Modems;*

2.2.40.7. *Dispositivos de fita;*

2.2.40.8. *Dispositivos multifuncionais;*

2.2.40.9. *Leitores de smart card;*

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

2.2.40.11. *Wi-Fi;*

2.2.40.12. *Adaptadores de rede externos;*

2.2.40.13. *Dispositivos MP3 ou smartphones;*

2.2.40.14. *Dispositivos Bluetooth;*

2.2.40.15. *Câmeras e Scanners.*

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

2.2.42. *Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;*

2.2.43. *Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;*

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

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

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

2.2.47. *Capacidade de bloquear execução de aplicativo que está em armazenamento externo;*

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

2.2.49. *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 à web;*

2.2.50. *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 à web;*

2.2.51. *Gerenciamento de Sistemas.*

3. Estações Mac OS X

3.1. Compatibilidade:

3.2. Mac OS X 10.11 (El Capitan);

3.3. Mac OS X 10.10 (Yosemite);

3.4. Mac OS X 10.9 (Mavericks).

3.5. Mac OS X 10.8 (Mountain Lion)

3.6. Mac OS X 10.7 (Lion)

3.7. Características:

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

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

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

3.7.4. Deve possuir suportes a notificações utilizando o Growl;

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

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

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

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

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

3.7.10. 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 tomar a partir da extensão do arquivo;

3.7.11. Capacidade de verificar somente arquivos novos e alterados;

3.7.12. Capacidade de verificar objetos usando heurística;

3.7.13. Capacidade de agendar uma pausa na verificação;

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

3.7.14.1. Perguntar o que fazer, ou;

3.7.14.2. Bloquear acesso ao objeto;

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

3.7.14.2.2. Caso positivo de desinfecção:

3.7.14.2.2.1. Restaurar o objeto para uso;

3.7.14.2.3. Caso negativo de desinfecção:

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

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

3.7.16. Capacidade de verificar arquivos de formato de email;

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

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

4. Estações de trabalho Linux

4.1. Compatibilidade:

4.1.1. Plataforma 32-bits:

4.1.1.1. Canaima 3;

4.1.1.2. Red Flag Desktop 6.0 SP2;

4.1.1.3. Red Hat Enterprise Linux 5.8 Desktop;

4.1.1.4. Red Hat Enterprise Linux 6.2 Desktop;

4.1.1.5. Fedora 16;

4.1.1.6. CentOS-6.2;

4.1.1.7. SUSE Linux Enterprise Desktop 10 SP4;

4.1.1.8. SUSE Linux Enterprise Desktop 11 SP2;

4.1.1.9. openSUSE Linux 12.1;

4.1.1.10. openSUSE Linux 12.2;

4.1.1.11. Debian GNU/Linux 6.0.5;

4.1.1.12. Mandriva Linux 2011;

4.1.1.13. Ubuntu 10.04 LTS;

4.1.1.14. Ubuntu 12.04 LTS.

4.1.2.Plataforma 64-bits:

4.1.2.1. Canaima 3;

4.1.2.2. Red Flag Desktop 6.0 SP2;

4.1.2.3. Red Hat Enterprise Linux 5.8;

4.1.2.4. Red Hat Enterprise Linux 6.2 Desktop;

4.1.2.5. Fedora 16;

4.1.2.6. CentOS-6.2;

4.1.2.7. SUSE Linux Enterprise Desktop 10 SP4;

4.1.2.8. SUSE Linux Enterprise Desktop 11 SP2;

4.1.2.9. openSUSE Linux 12.1;

4.1.2.10. openSUSE Linux 12.2;

4.1.2.11. Debian GNU/Linux 6.0.5;

4.1.2.12. Ubuntu 10.04 LTS;

4.1.2.13. Ubuntu 12.04 LTS.

4.2. Características:

4.2.1. Deve prover as seguintes proteções:

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

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

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

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

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

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

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

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

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

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

4.2.6. Capacidade de verificar objetos usando heurística;

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

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

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

5. Servidores Windows

5.1. Compatibilidade:

5.2. Plataforma 32-bits:

5.2.1. Microsoft Windows Server 2003 Standard / Enterprise (SP2);

5.2.2. Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);

5.2.3. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

5.2.4. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).

5.3. Plataforma 64-bits:

5.3.1. Microsoft Windows Server 2003 Standard / Enterprise (SP2);

5.3.2. Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);

5.3.3. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

5.3.4. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

5.3.5. Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);

5.3.6. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

5.3.7. Microsoft Windows Storage Server 2008 R2;

5.3.8. Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);

5.3.9. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

5.3.10. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

5.3.11. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;

5.3.12. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;

5.3.13. Microsoft Windows Storage Server 2012 (Todas edições);

5.3.14. Microsoft Windows Storage Server 2012 R2 (Todas edições);

5.3.15. Microsoft Windows Hyper-V Server 2012;

5.3.16. Microsoft Windows Hyper-V Server 2012 R2.

5.4. Características:

5.4.1. Deve prover as seguintes proteções:

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

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

5.4.1.3. Firewall com IDS;

5.4.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

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

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

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

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

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

5.4.4.3. Leitura de configurações;

5.4.4.4. Modificação de configurações;

5.4.4.5. Gerenciamento de Backup e Quarentena;

5.4.4.6. Visualização de relatórios;

5.4.4.7. Gerenciamento de relatórios;

5.4.4.8. Gerenciamento de chaves de licença;

5.4.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

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

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

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

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

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

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

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

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

5.4.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

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

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

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

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

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

5.4.17. Capacidade de verificar somente arquivos novos e alterados;

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

5.4.19. Capacidade de verificar objetos usando heurística;

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

5.4.21. Capacidade de agendar uma pausa na verificação;

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

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

5.4.23.1. Perguntar o que fazer, ou;

5.4.23.2. Bloquear acesso ao objeto;

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

5.4.23.2.2. Caso positivo de desinfecção:

5.4.23.2.2.1. Restaurar o objeto para uso;

5.4.23.2.3. Caso negativo de desinfecção:

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

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

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

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

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

6. *Servidores Linux*

6.1. Compatibilidade: Plataforma 32-bits:

6.1.1.Red Hat Enterprise Linux Server 5.x;

6.1.2.Red Hat® Enterprise Linux® Server 6.x (6.0 - 6.6);

6.1.3.CentOS 6.x (6.0 - 6.6);

6.1.4.SUSE® Linux Enterprise Server 11 SP3;

6.1.5.Ubuntu Server 12.04 LTS;

6.1.6.Ubuntu Server 14.04 LTS;

6.1.7.Ubuntu Server 14.10;

6.1.8.Oracle Linux 6.5;

6.1.9.Debian GNU/Linux 7.5, 7.6, 7.7;

6.1.10. openSUSE 13.1.

6.1.11. Plataforma 64-bits:

6.1.12. Red Hat Enterprise Linux Server 5.x;

6.1.13. Red Hat Enterprise Linux Server 6.x (6.0 - 6.6);

6.1.14. Red Hat Enterprise Linux Server 7;

6.1.15. CentOS-6.x (6.0 - 6.6);

6.1.16. CentOS-7.0;

6.1.17. SUSE Linux Enterprise Server 11 SP3;

6.1.18. SUSE Linux Enterprise Server 12;

6.1.19. Novell Open Enterprise Server 11 SP1;

6.1.20. Novell Open Enterprise Server 11 SP2;

6.1.21. Ubuntu Server 12.04 LTS;

6.1.22. Ubuntu Server 14.04 LTS;

6.1.23. Ubuntu Server 14.10;

6.1.24. Oracle Linux 6.5;

6.1.25. Oracle Linux 7.0;

6.1.26. Debian GNU/Linux 7.5, 7.6, 7.7;

6.1.27. openSUSE® 13.1.

7. Características:

7.1.1. Deve prover as seguintes proteções:

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

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

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

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

7.1.2.2. 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;

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

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

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

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

7.1.5. 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 tomar a partir da extensão do arquivo;

7.1.6. Capacidade de verificar objetos usando heurística;

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

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

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

8. Servidores Novell Netware:

8.1. ***Compatibilidade:***

8.1.1. Novell Netware 5.x Support Pack 6 ou superior;

8.1.2. Novell Netware 6.0 Support Pack 3 ou superior;

8.1.3. Novell Netware 6.5 Support Pack 3 ou superior.

8.2. ***Características:***

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

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

8.2.3. Capacidade de realizar update de maneira automatica, via internet ou LAN;

8.2.4. Capacidade de fazer um rollback das vacinas;

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

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

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

8.2.8. Capacidade de notificar o administrador de varreduras concluidas e sobre objetos maliciosos encontrados no servidor, utilizando a rede Novell ou e-mail.

9. Smartphones e tablets

9.1. ***Compatibilidade:***

9.1.1. Apple iOS 7.0 – 8.X;

9.1.2. Windows Phone 8.1;

9.1.3. Android OS 2.3 – 5.1.

9.2. Características:

9.2.1. Deve prover as seguintes proteções:

9.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

9.2.1.1.1. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

9.2.1.1.2. Arquivos abertos no smartphone;

9.2.1.1.3. Programas instalados usando a interface do smartphone

9.2.1.2. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

9.2.2. Deverá isolar em área de quarentena os arquivos infectados;

9.2.3. Deverá atualizar as bases de vacinas de modo agendado;

9.2.4. Deverá bloquear spams de SMS através de Black lists;

9.2.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;

9.2.6. Capacidade de desativar por política:

Wi-fi;

Câmera;

Bluetooth.

9.2.7. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

9.2.8. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

9.2.9. Deverá ter firewall pessoal (Android);

9.2.10. Capacidade de tirar fotos quando a senha for inserida incorretamente;

9.2.11. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

9.2.12. Capacidade de enviar comandos remotamente de:

- *Localizar;*
- *Bloquear.*

9.2.13. Capacidade de detectar Jailbreak em dispositivos iOS;

9.2.14. Capacidade de bloquear o acesso a site por categoria em dispositivos;

9.2.15. Capacidade de bloquear o acesso a sites phishing ou malicioso;

9.2.16. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;

9.2.17. Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído;

9.2.18. Capacidade de configurar White e blacklist de aplicativos;

9.2.19. Capacidade de localizar o dispositivo quando necessário;

9.2.20. Permitir atualização das definições quando estiver em "roaming";

9.2.21. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

9.2.22. Capacidade de enviar URL de instalação por e-mail;

9.2.23. Capacidade de fazer a instalação através de um link QRCode;

9.2.24. Capacidade de executar as seguintes ações caso a desinfecção falhe:

- *Deletar;*
- *Ignorar;*
- *Quarentenar;*
- *Perguntar ao usuário.*

ANEXO II DO TERMO DE REFERÊNCIA

PLANILHA ORÇAMENTÁRIA

ITEM	***ESPECIFICAÇÃO MÍNIMAS***	***MARCA/ Modelo***	***QUANT.***	***VALOR UNIT.***	***VALOR TOTAL***
01	***LICENÇA PARA USO DE SOFTWARE (ANTIVÍRUS):*** *Licenciamento perpétuo; Linguagem: português do Brasil; Recursos inclusos: Antimalware; Firewall; Proteção assistida em nuvem; Controle de aplicativos; Lista branca de aplicativos; Monitoramento e controle de acesso à internet (WEB); Gerenciamento e controle de dispositivos móveis para acesso da rede corporativa; Proteção de servidores de arquivos em plataformas Windows, Linux ou FreeBSB; Segurança de endpoints móveis (tablets e smartphones); Dados corporativos e pessoais separados e armazenados em contêineres criptografados; Gerenciamento de Sistemas; cifrado; Centralização do gerenciamento das tarefas a partir de 01 (um) console; Assistência técnica remota 8x5; Conteúdo da embalagem (box): CD de mídia, código de ativação (chave) para 11 licenças e manual do usuário; Todas as licenças terão validade de 03 (três) anos de atualizações.*		***11***		

	Referência: Kaspersky Endpoint Security For Business Advanced ou similar;				

ANEXO III DO TERMO DE REFERÊNCIA

GERENCIAMENTO DE RISCO

1 – RISCOS DO PROCESSO DE CONTRATAÇÃO			
RISCO 1			
Risco:	**Demora na conclusão do procedimento licitatório**	**Probabilidade**	Moderada
Id	**Dano**		
1	Atraso na licitação para atender as demandas da CMI.		
Id	**Ação Preventiva**	**Responsável**	
1	Acompanhamento junto aos órgãos envolvidos e à equipe responsável pela licitação visando dar celeridade no andamento do processo.	Equipe de planejamento.	
Id	**Ação de Contingência**	**Responsável**	
1	Cobrança junto à área responsável e agilidade na avaliação das propostas técnicas.	Equipe de planejamento.	
RISCO 2			
Risco:	**Atraso na instalação e/ou renovação de licença**	**Probabilidade**	Baixa
Id	**Dano**		
1	Atraso na entrega do software.		
Id	**Ação Preventiva**	**Responsável**	
1	Cobrar o fornecedor a instalação e/ou atualização em tempo hábil.	Equipe de planejamento.	
Id	**Ação de Contingência**	**Responsável**	
1	Suspender o pagamento, advertir a contratada e aplicar as penalidades previstas e cabíveis.	Equipe de planejamento e autoridade superior	
RISCO 3			
Risco:	**Atraso na aquisição das 2 (duas) estações de trabalho**	**Probabilidade**	Moderada
Id	**Dano**		
1	Instalação de software em duas estações de trabalho em período divergente dos demais. Possibilidade da perca da garantia.		
Id	**Ação Preventiva**	**Responsável**	
1	Agilidade no procedimento licitatório.	Equipe de planejamento	
Id	**Ação de Contingência**	**Responsável**	
1	Garantir contratualmente a garantia integral dos computadores remanescentes	Equipe de Contratos e Jurídico.	