PREFEITURA MUNICIPAL DE CONGONHAS
CIDADE DOS PROFETAS

CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº. PMC/113/2017

Nº PMC/2206/2017
PRC/179/2017
PREGÃO: PMC/077/2017

"Contratação de empresa especializada na prestação de serviços de licenciamento de Antivírus com direito a atualização e suporte técnico para estações de trabalho, servidores de arquivos, incluindo suporte, remoto e/ou in loco e atualização de versão para utilização no parque tecnológico do município de Congonhas-MG e Aquisição de 01 (*um*) Servidor de Administração do Sistema de Antivírus."

Termo de contrato de prestação de serviços de empresa licenciamento de Antivírus com direito a atualização e suporte técnico para estações de trabalho, servidores de arquivos, incluindo suporte, remoto e/ou in loco e atualização de versão para utilização no parque tecnológico e Aquisição de 01 (*um*) Servidor de Administração do Sistema de Antivírus, que fazem entre si o MUNICÍPIO DE CONGONHAS, CNPJ nº 16.752.446/0001-02, neste ato representado por seu Prefeito Municipal Sr. José de Freitas Cordeiro, que por força do Decreto nº 5.936 de 07 de fevereiro de 2014 passa a integrar o presente contrato o(s) Secretário(s) Gestor(es), doravante denominado CONTRATANTE, e a empresa MICROHARD INFORMÁTICA LTDA - EPP, CNPJ nº 42.832.691/0001-30, localizado na Rua República da Argentina, nº 520, 2º andar, Bairro Sion, CEP. 30.315-490, Belo Horizonte, neste ato representado pelo Sr. José Glicério Ruas Alves, CPF nº 173.863.226-15, C.I nº M-529.162, doravante denominada CONTRATADA, perante as testemunhas abaixo assinadas, firmam o presente contrato, decorrente do processo licitatório nº. PRC/179/2017, Pregão Presencial nº 077/2017, Processo Administrativo nº PMC/2206/2017 e que se regerá pelas Leis nº 10.520/02 e 8.666/93 e posteriores alterações, atendidas as cláusulas e condições que se enunciam a seguir:

CLAUSULA I - DO OBJETO

1.1. Contratação de empresa licenciamento de Antivírus com direito a atualização e suporte técnico para estações de trabalho, servidores de arquivos, incluindo suporte, remoto e/ou in loco e atualização de versão para utilização no parque tecnológico do município de Congonhas-MG e Aquisição de 01 (*um*) Servidor de Administração do Sistema de Antivírus, conforme especificações constantes no Termo de Referência, que integra o presente Edital.

CLÁUSULA II - DO OBJETIVO

2.1. Compra de licenças de Antivírus com direito a atualizações e suporte técnico pelo período de 12(doze) meses para estações de trabalho, servidores de arquivos, incluindo

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

suporte, remoto e/ou in loco, e atualização de versão para utilização no parque tecnológico para o Município de Congonhas, pelo período de 12(doze) meses.

2.2. Aquisição de 01 (*um*) servidor de administração do sistema de antivírus.

2.3. A Solução de Tecnologia da Informação e Comunicação, é composta pelo seguinte objeto:

Item	Descrição	Quantidade
01	Compra de licenças do Antivírus coorporativo	750
02	Compra de Servidor para administração do sistema de AntiVírus	01

CLAUSULA III – DO PREÇO, DO PAGAMENTO E REAJUSTE

3.1. O preço da prestação de serviços licitado será o mesmo apresentado no mapa de julgamento da licitante vencedora, constante do Pregão Presencial nº. PMC/077/2017.

3.2. O valor global do presente contrato é de **R$ 114.000,00** (cento e quatorze mil reais).

3.3. O pagamento decorrente da aquisição do objeto será efetivado no prazo de 30 (trinta) dias contados da implantação, configuração do servidor e disponibilização do software de antivírus no referido equipamento, acompanhado das respectivas chaves de licença para instalação, através de depósito na conta corrente da contratada, a ser informada no ato da assinatura do contrato, mediante a apresentação das notas fiscais devidamente atestadas pelo setor responsável, bem como das cópias da **CND do INSS e do CRF do FGTS e CNDT.**

3.4. Os pagamentos referentes à aquisição do servidor e às licenças dos softwares serão efetuados em parcela única no prazo e condições descritos no item anterior, devidamente atestados pelo órgão de execução.

3.5. Os valores pertinentes ao serviço de implantação serão pagos logo após a efetiva prestação dos serviços.

3.6. O preço a ser cobrado pelas licenças do software de antivírus será fixo e irreajustável na vigência do contrato.

3.7. O preço ofertado para conversão de dados, implantação, capacitação de usuários, manutenção e suporte técnico, será pago em parcela única, e por isto não será reajustado.

3.8. O preço ofertado para cessão do direito de uso poderá ser reajustado pelo índice IGP-M, ou na falta desse, pelo índice que o vier substituir, caso haja interesse das partes da prorrogação de prazo contratual, após 12 (doze) meses de prestação de serviço, tendo por base a data de assinatura do contrato, mediante requerimento da CONTRATADA, com prazo de até 30 (trinta) dias anteriores ao reajuste anual.

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

3.9. Os preços serão reajustados após cada ano de vigência do contrato, pela variação do IGPM ou outro índice oficial que venha a substituí-lo.

3.9.1. O reajuste de que trata o item anterior somente incidirá a partir do 1º dia do 2º ano de vigência do contrato.

3.9.2. Não sendo conhecido o índice do mês do reajuste, poderá ser utilizado o índice do mês anterior.

3.9.3. De acordo com o Decreto nº 5.832/2013, aplicar-se-ão as seguintes regras à contratada;

a) O reajuste deve ser concedido mediante requerimento da parte contratada, em observância as regras do respectivo contrato e instrumento convocatório;

b) Não será aplicado o reajuste após prorrogação contratual, se na celebração desse aditivo a parte contratada foi omissa no exercício de seu direito;

c) Inaplicável o reajuste referente o contrato expirado.

CLÁUSULA IV – ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

4.1. Registro de preços de licenças de Antivírus. Características gerais:

4.1.1. Todas as licenças fornecidas terão validade de 12 (*doze*) meses para atualizações inerentes ao produto;

4.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus, quanto do software;

4.1.3. As atualizações deverão ser disponibilizadas através de site na Internet, ou através do próprio software;

4.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para o CONTRATANTE além daquele já cotado na proposta;

CLÁUSULA V – SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA

5.1. Servidor de Administração

5.1.1. Compatibilidade mínima:

5.1.1.1. Microsoft Windows 10 Pro 32-bit / 64-bit, Microsoft Windows 10 Enterprise 32-bit / 64-bit,

5.1.1.2. Microsoft Windows 10 Education 32-bit / 64-bit

5.1.1.3. Microsoft Windows 8.1 Pro 32-bit / 64-bit

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

5.1.1.4. Microsoft Windows 8.1 Enterprise 32-bit / 64-bit
5.1.1.5. Microsoft Windows 8 Pro 32-bit / 64-bit
5.1.1.6. Microsoft Windows 8 Enterprise 32-bit / 64-bit
5.1.1.7. Microsoft Windows 7 Professional SP1 32-bit / 64-bit
5.1.1.8. Microsoft Windows 7 Enterprise SP1 32-bit / 64-bit
5.1.1.9. Microsoft Windows 7 Ultimate SP1 32-bit / 64-bit
5.1.1.10. Microsoft Windows 7 Professional 32-bit / 64-bit
5.1.1.11. Microsoft Windows 7 Enterprise 32-bit / 64-bit
5.1.1.12. Microsoft Windows 7 Ultimate 32-bit / 64-bit
5.1.1.13. Microsoft Small Business Server 2008 Standard 64-bit
5.1.1.14. Microsoft Small Business Server 2008 Premium 64-bit
5.1.1.15. Microsoft Small Business Server 2011 Essentials 64-bit
5.1.1.16. Microsoft Small Business Server 2011 Premium Add-on 64-bit
5.1.1.17. Microsoft Small Business Server 2011 Standard 64-bit
5.1.1.18. Microsoft Windows Server 2008 Datacenter SP1 32-bit / 64-bit
5.1.1.19. Microsoft Windows Server 2008 Enterprise SP1 32-bit / 64-bit
5.1.1.20. Microsoft Windows Server 2008 Foundation SP2 32-bit / 64-bit
5.1.1.21. Microsoft Windows Server 2008 SP1 Server Core 32-bit / 64-bit
5.1.1.22. Microsoft Windows Server 2008 Standard SP1 32-bit / 64-bit
5.1.1.23. Microsoft Windows Server 2008 Standard 32-bit / 64-bit
5.1.1.24. Microsoft Windows Server 2008 Enterprise 32-bit / 64-bit
5.1.1.25. Microsoft Windows Server 2008 Datacenter 32-bit / 64-bit
5.1.1.26. Microsoft Windows Server 2008 R2 Server Core64-bit
5.1.1.27. Microsoft Windows Server 2008 R2 Datacenter 64-bit
5.1.1.28. Microsoft Windows Server 2008 R2 Datacenter SP1 64-bit
5.1.1.29. Microsoft Windows Server 2008 R2 Enterprise 64-bit
5.1.1.30. Microsoft Windows Server 2008 R2 Enterprise SP1 64-bit
5.1.1.31. Microsoft Windows Server 2008 R2 Foundation 64-bit
5.1.1.32. Microsoft Windows Server 2008 R2 Foundation SP1 64-bit
5.1.1.33. Microsoft Windows Server 2008 R2 SP1 Core Mode 64-bit
5.1.1.34. Microsoft Windows Server 2008 R2 Standard 64-bit
5.1.1.35. Microsoft Windows Server 2008 R2 Standard SP1 64-bit
5.1.1.36. Microsoft Windows Server 2012 Server Core 64-bit
5.1.1.37. Microsoft Windows Server 2012 Datacenter 64-bit

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

5.1.1.38. Microsoft Windows Server 2012 Essentials 64-bit

5.1.1.39. Microsoft Windows Server 2012 Foundation 64-bit

5.1.1.40. Microsoft Windows Server 2012 Standard 64-bit

5.1.1.41. Microsoft Windows Server 2012 R2 Server Core64-bit

5.1.1.42. Microsoft Windows Server 2012 R2 Datacenter 64-bit

5.1.1.43. Microsoft Windows Server 2012 R2 Essentials 64-bit

5.1.1.44. Microsoft Windows Server 2012 R2 Foundation 64-bit

5.1.1.45. Microsoft Windows Server 2012 R2 Standard 64-bit

5.2. Console de Administração

5.2.1. Compatibilidade mínima:

5.2.1.1. Microsoft Windows Server 2003

5.2.1.2. Microsoft Windows Server 2008

5.2.1.3. Microsoft Windows Server 2008 R2

5.2.1.4. Microsoft Windows Vista

5.2.1.5. Sistemas operacionais relacionados no item 15.1.1

5.3. Suportar as seguintes plataformas virtuais:

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

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

5.3.3. Citrix XenServer 6.1, 6.2.

5.4. Características mínimas obrigatórias:

5.4.1. A console deve ser acessada via WEB (HTTPS) e MMC;

5.4.2. Console deve ser baseada no modelo cliente/servidor;

5.4.3. Compatibilidade com Windows *FailoverClustering* ou outra solução de alta disponibilidade;

5.4.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

5.4.5. Console deve ser totalmente integrada com suas funções e módulos;

5.4.6. 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;

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

5.4.8. 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;

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

5.4.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

5.4.10. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

5.4.11. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

5.4.12. Capacidade de instalar remotamente a solução de segurança e qualquer "*app*" em smartphones e tablets de sistema iOS, Android e Windows;

5.4.13. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

5.4.14. 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;

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

5.4.16. Capacidade de gerenciar smartphones e tablets (*Windows Phone, Android e iOS*) protegidos pela solução de segurança;

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

5.4.18. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

5.4.19. 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;

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

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

5.4.22. 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.

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

5.4.24. 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;

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

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

5.4.26. 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;

5.4.27. 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;

5.4.28. Capacidade de agrupamento de máquina por características comuns entre as mesmas, atendendo a no mínimo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, agrupar as máquinas por versão do sistema operacional, por arquitetura do sistema operacional, por nome de aplicação, fabricante, tipo de máquina virtual, processador e placa de rede;

5.4.29. 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;

5.4.30. Deve fornecer as seguintes informações dos computadores:

5.4.30.1. Se o antivírus está instalado;

5.4.30.2. Se o antivírus está iniciado;

5.4.30.3. Se o antivírus está atualizado;

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

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

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

5.4.30.7. Versão do antivírus instalado na máquina;

5.4.30.8. Se é necessário reiniciar o computador para aplicar mudanças;

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

5.4.30.10. Quantidade de vírus encontrados (*contador*) na máquina;

5.4.30.11. Nome do computador;

5.4.30.12. Domínio ou grupo de trabalho do computador;

5.4.30.13. Data e horário da última atualização de vacinas;

5.4.30.14. Sistema operacional com Service Pack;

5.4.30.15. Quantidade de processadores;

5.4.30.16. Quantidade de memória RAM;

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

5.4.30.18. Endereço IP;

José de Freitas Cardeiro
Prefeito Municipal de Congonhas

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

5.4.30.20. Atualizações do Windows Updates instaladas;

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

5.4.30.22. Vulnerabilidades de aplicativos instalados na máquina;

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

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

5.4.32.1. Alteração de Gateway Padrão;

5.4.32.2. Alteração de subrede;

5.4.32.3. Alteração de domínio;

5.4.32.4. Alteração de servidor DHCP;

5.4.32.5. Alteração de servidor DNS;

5.4.32.6. Alteração de servidor WINS;

5.4.32.7. Alteração de subrede;

5.4.32.8. Resolução de Nome;

5.4.32.9. Disponibilidade de endereço de conexão SSL;

5.4.33. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

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

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

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

5.4.37. 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;

5.4.38. 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;

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

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

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

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

5.4.43. 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;

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

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

5.4.46. 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.

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

5.4.48. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

5.4.49. Capacidade de realizar conexão de área remota mediante o aceite do usuário.

CLÁUSULA VI – ESTAÇÕES WINDOWS

6.1. Compatibilidade mínima:

6.1.1. Microsoft Windows Embedded 8.0 Standard x64;

6.1.2. Microsoft Windows Embedded 8.1 Industry Pro x64;

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

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

6.1.5. Microsoft Windows Vista x86 / x64SP2 e posterior;

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

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

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

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

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

6.2. Características mínimas obrigatórias:

6.2.1. Deve prover as seguintes proteções:

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

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

6.2.1.3. Antivírus de E-mail (*módulo para verificação de anexos de e-mails recebidos e enviados*);

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

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

6.2.1.6. Firewall com IDS;

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

6.2.1.8. Controle de dispositivos externos;

6.2.1.9. Controle de acesso a sites por categoria;

6.2.1.10. Controle de acesso a sites por horário;

6.2.1.11. Controle de acesso a sites por usuários;

6.2.1.12. Controle de execução de aplicativos;

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

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

6.2.3. 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);

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

6.2.5. 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;

6.2.6. 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;

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

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

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

6.2.9. 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;

6.2.10. Capacidade de verificar somente arquivos novos e alterados;

6.2.11. Capacidade de verificar objetos usando heurística;

6.2.12. Capacidade de agendar uma pausa na verificação;

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

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

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

6.2.15.1. Perguntar o que fazer, ou;

6.2.15.2. Bloquear acesso ao objeto;

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

6.2.15.4. Caso positivo de desinfecção:

6.2.15.4.1. Restaurar o objeto para uso;

6.2.15.5. Caso negativo de desinfecção:

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

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

6.2.17. 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);

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

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

6.2.20. Capacidade de verificar tráfego em browsers;

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

6.2.21.1. Perguntar o que fazer, ou;

6.2.21.2. Bloquear o e-mail;

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

6.2.21.2.2. Caso positivo de desinfecção:

6.2.21.2.2.1. Restaurar o e-mail para o usuário;

6.2.21.2.3. Caso negativo de desinfecção:

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

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

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

6.2.23. Possibilidade de verificar somente e-mails recebidos;

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

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

6.2.26. Deve ter suporte total ao protocolo IPv6;

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

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

6.2.28.1. Perguntar o que fazer, ou;

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

6.2.28.3. Permitir acesso ao objeto;

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

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

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

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

6.2.31. 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;

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

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

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

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

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

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

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

6.2.36.2. 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.

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

6.2.37.1. Discos de armazenamento locais;

6.2.37.2. Armazenamento removível;

6.2.37.3. Impressoras;

6.2.37.4. CD/DVD;

6.2.37.5. Drives de disquete;

6.2.37.6. Modems;

6.2.37.7. Dispositivos de fita;

6.2.37.8. Dispositivos multifuncionais;

6.2.37.9. Leitores de smartcard;

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

6.2.37.11. Wi-Fi;

6.2.37.12. Adaptadores de rede externos;

6.2.37.13. Dispositivos MP3 ou smartphones;

6.2.37.14. Dispositivos Bluetooth;

6.2.37.15. Câmeras e Scanners.

6.2.38. 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;

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

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

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

6.2.42. 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;

6.2.43. Capacidade de limitar a execução de aplicativos por *hash MD5*, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo,

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

fabricante/desenvolvedor e categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

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

6.2.45. 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;

6.2.46. 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;

6.2.47. Deve ter a capacidade de detectar, nativamente, ataques originados por *ransomware*. A detecção para este tipo de malware deve basear-se não apenas nas informações do banco de dados de definições de vírus, mas também no comportamento do malware; mesmo que ainda não tenha sido desenvolvida, pelo fabricante, vacina para combater o mesmo.

6.2.48. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa, com outras regras de firewall até controle de aplicativos, dispositivos e acesso à web.

CLÁUSULA VII – ESTAÇÕES MAC OS X

7.1 Compatibilidade mínima:

7.1.2. Mac OS X 10.11 (El Capitan);

7.1.3. Mac OS X 10.10 (Yosemite);

7.1.4. Mac OS X 10.9 (Mavericks).

7.1.5. Mac OS X 10.8 (Mountain Lion)

7.1.6. Mac OS X 10.7 (Lion)

7.2. Características mínimas obrigatórias:

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

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

7.2.4. 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;

7.2.5. Deve possuir suporte a notificações utilizando o Growl;

7.2.6. 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);

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

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

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

7.2.9. 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;

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

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

7.2.12. Capacidade de verificar somente arquivos novos e alterados;

7.2.13. Capacidade de verificar objetos usando heurística;

7.2.14. Capacidade de agendar uma pausa na verificação;

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

7.2.15.1. Perguntar o que fazer, ou;

7.2.15.2. Bloquear acesso ao objeto;

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

7.2.15.2.2. Caso positivo de desinfecção:

7.2.15.2.2.1. Restaurar o objeto para uso;

7.2.15.2.3. Caso negativo de desinfecção:

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

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

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

7.2.18. 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;

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

CLÁUSULA VIII – ESTAÇÕES DE TRABALHO LINUX

8.1. Compatibilidade mínima:

8.1.1. Plataforma 32-bits:

8.1.1.1. Canaima 3;

8.1.1.2. Red Flag Desktop 6.0 SP2;

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

8.1.1.3. Red Hat Enterprise Linux 5.8 Desktop;
8.1.1.4. Red Hat Enterprise Linux 6.2 Desktop;
8.1.1.5. Fedora 16;
8.1.1.6. CentOS-6.2;
8.1.1.7. SUSE Linux Enterprise Desktop 10 SP4;
8.1.1.8. SUSE Linux Enterprise Desktop 11 SP2;
8.1.1.9. Open SUSE Linux 12.1;
8.1.1.10. OpenSUSE Linux 12.2;
8.1.1.11. Debian GNU/Linux 6.0.5;
8.1.1.12. Mandriva Linux 2011;
8.1.1.13. Ubuntu 10.04 LTS;
8.1.1.14. Ubuntu 12.04 LTS.

8.1.2. Plataforma 64-bits:

8.1.2.1. Canaima 3;
8.1.2.2. Red Flag Desktop 6.0 SP2;
8.1.2.3. Red Hat Enterprise Linux 5.8;
8.1.2.4. Red Hat Enterprise Linux 6.2 Desktop;
8.1.2.5. Fedora 16;
8.1.2.6. CentOS-6.2;
8.1.2.7. SUSE Linux Enterprise Desktop 10 SP4;
8.1.2.8. SUSE Linux Enterprise Desktop 11 SP2;
8.1.2.9. Open SUSE Linux 12.1;
8.1.2.10. OpenSUSE Linux 12.2;
8.1.2.11. Debian GNU/Linux 6.0.5;
8.1.2.12. Ubuntu 10.04 LTS;
8.1.2.13. Ubuntu 12.04 LTS.

8.2. Características mínimas obrigatórias:

8.2.1. Deve prover as seguintes proteções:

8.2.1.1. Antivírus de arquivos residente (*anti-spyware, anti-trojan, anti-malware, etc*) que verifique qualquer arquivo criado, acessado ou modificado;
8.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

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

8.2.3.1. 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;

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

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

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

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

8.2.6. 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;

8.2.7. Capacidade de verificar objetos usando heurística;

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

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

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

CLÁUSULA IX – SERVIDORES WINDOWS

9.1. Compatibilidade mínima:

9.1.1. Plataforma 32-bits:

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

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

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

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

9.1.2. Plataforma 64-bits:

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

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

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

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

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

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

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

9.1.2.7. Microsoft Windows Storage Server 2008 R2;

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

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

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

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

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

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

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

9.1.2.15. Microsoft Windows Hyper-V Server 2012;

9.1.2.16. Microsoft Windows Hyper-V Server 2012 R2.

9.2. Características mínimas obrigatórias:

9.2.1. Deve prover as seguintes proteções:

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

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

9.2.1.3. Firewall com IDS;

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

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

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

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

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

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

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

9.2.4.3. Leitura de configurações;

9.2.4.4. Modificação de configurações;

9.2.4.5. Gerenciamento de Backup e Quarentena;

9.2.4.6. Visualização de relatórios;

9.2.4.7. Gerenciamento de relatórios;

9.2.4.8. Gerenciamento de chaves de licença;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

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

9.2.17. Capacidade de verificar somente arquivos novos e alterados;

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

9.2.19. Capacidade de verificar objetos usando heurística;

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

9.2.21. Capacidade de agendar uma pausa na verificação;

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

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

9.2.23.1. Perguntar o que fazer, ou;

9.2.23.2. Bloquear acesso ao objeto;

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

9.2.23.2.2. Caso positivo de desinfecção:

9.2.23.2.2.1. Restaurar o objeto para uso;

9.2.23.2.3. Caso negativo de desinfecção:

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

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

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

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

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

9.2.28. Deve ter a capacidade de detectar, nativamente, ataques originados por ransomware. A detecção para este tipo de malware deve basear-se não apenas nas informações do banco de dados de definições de vírus, mas também no comportamento do malware; mesmo que ainda não tenha sido desenvolvida, pelo fabricante, vacina para combater o mesmo.

CLÁUSULA X – SERVIDORES LINUX

10.1.Compatibilidade mínima:

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

Plataforma 32-bits:

10.1.1. Red Hat Enterprise Linux Server 5.x;

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

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

10.1.4. SUSE® Linux Enterprise Server 11 SP3;

10.1.5. Ubuntu Server 12.04 LTS;

10.1.6. Ubuntu Server 14.04 LTS;

10.1.7. Ubuntu Server 14.10;

10.1.8. Oracle Linux 6.5;

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

10.1.10. openSUSE 13.1.

Plataforma 64-bits:

10.1.11. Red Hat Enterprise Linux Server 5.x;

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

10.1.13. Red Hat Enterprise Linux Server 7;

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

10.1.15. CentOS-7.0;

10.1.16. SUSE Linux Enterprise Server 11 SP3;

10.1.17. SUSE Linux Enterprise Server 12;

10.1.18. Novell Open Enterprise Server 11 SP1;

10.1.19. Novell Open Enterprise Server 11 SP2;

10.1.20. Ubuntu Server 12.04 LTS;

10.1.21. Ubuntu Server 14.04 LTS;

10.1.22. Ubuntu Server 14.10;

10.1.23. Oracle Linux 6.5;

10.1.24. Oracle Linux 7.0;

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

10.1.26. openSUSE® 13.1.

10.2.Características mínimas obrigatórias:

10.2.1. Deve prover as seguintes proteções:

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

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

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

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

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

10.2.2.2. 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;

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

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

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

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

10.2.5. 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;

10.2.6. Capacidade de verificar objetos usando heurística;

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

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

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

CLÁUSULA XI – SMARTPHONES E TABLETS

11.1.Compatibilidade mínima:

11.1.1. Apple iOS 7.0 – 8.X;

11.1.2. Windows Phone 8.1;

11.1.3. Android OS 4.x e superiores.

11.2.Características mínimas obrigatórias:

11.2.1. Deve prover as seguintes proteções:

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

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

11.2.1.1.1. 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;

11.2.1.1.2. Arquivos abertos no smartphone;

11.2.1.1.3. Programas instalados usando a interface do smartphone

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

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

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

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

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

11.2.6. Capacidade de desativar por política:

- Wi-fi;
- Câmera;
- Bluetooth.

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

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

11.2.9. Deverá ter firewall pessoal (Android);

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

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

11.2.12. Capacidade de enviar comandos remotamente de:

- Localizar;
- Bloquear.

11.2.13. Capacidade de detectar Jailbreak em dispositivos iOS, Root em Android e Interop em Windows Phone;

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

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

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

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

11.2.18. Capacidade de configurar White e blacklist de aplicativos;

11.2.19. Capacidade de localizar o dispositivo quando necessário;

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

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

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

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

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

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

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

CLÁUSULA XII – GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM)

12.1.Compatibilidade mínima com os seguintes dispositivos:

12.1.1. Dispositivos conectados através do Microsoft Exchange ActiveSync:
12.1.1.1. Windows Phone;
12.1.1.2. Android.
12.1.2. Dispositivos com suporte ao Apple PushNotification (APNs).
12.1.2.1. Apple iOS 7.0 ou superior.

12.2.Características mínimas obrigatórias:

12.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
12.2.2. Capacidade de ajustar as configurações de:
12.2.2.1. Sincronização de e-mail;
12.2.2.2. Uso de aplicativos;
12.2.2.3. Senha do usuário;
12.2.2.4. Criptografia de dados;
12.2.2.5. Conexão de mídia removível.
12.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
12.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS;
12.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
12.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS;

CLÁUSULA XIII – CRIPTOGRAFIA

13.1.Compatibilidade:

13.1.1. Microsoft Windows Vista Business/Enterprise/Ultimate SP2;
13.1.2. Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2;
13.1.3. Microsoft Windows 7 Professional/Enterprise/Ultimate;
13.1.4. Microsoft Windows 7 Professional/Enterprise/Ultimate x64;
13.1.5. Microsoft Windows 8 Professional/Enterprise;
13.1.6. Microsoft Windows 8 Professional/Enterprise x64;
13.1.7. Microsoft Windows 8.1 Professional / Enterprise;
13.1.8. Microsoft Windows 8.1 Professional / Enterprise x64;

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

13.1.9. Microsoft Windows 10 Pro x86 / x64;
13.1.10. Microsoft Windows 10 Enterprise x86 /x64.

13.2. Características mínimas obrigatórias:

13.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;
13.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
13.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
13.2.4. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;
13.2.5. Permitir criar vários usuários de autenticação pré-boot;
13.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
13.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
13.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
13.2.7.2. Criptografar todos os arquivos individualmente;
13.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
13.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
13.2.8. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;
13.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
13.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
13.2.11. Verificar compatibilidade de hardware antes de aplicar a criptografia;
13.2.12. Possibilitar estabelecer parâmetros para a senha de criptografia;
13.2.13. Bloquear o reuso de senhas;
13.2.14. Bloquear a senha após um número de tentativas pré-estabelecidas;
13.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
13.2.16. Permitir criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo
13.2.17. Permitir criptografar as seguintes pastas pré-definidas: "meus documentos", "Favoritos", "Desktop", "Arquivos temporários" e "Arquivos do outlook";
13.2.18. Permitir utilizar variáveis de ambiente para criptografar pastas customizadas;
13.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, arquivos de audio, etc;
13.2.20. Permitir criar um grupo de extensões de arquivos a serem criptografados;
13.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
13.2.22. Permitir criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

CLÁUSULA XVI – GERENCIAMENTO DE SISTEMAS

A Solução deve possuir as seguintes características mínimas obrigatórias:

14.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;
14.2. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
14.3. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
14.4. Possuir tecnologia com a possibilidade de criar regras de quais tipos de dispositivos podem ter acessos a recursos da rede;
14.5. Capacidade de gerenciar licenças de softwares de terceiros;
14.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
14.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, servicetag, número de identificação e outros;
14.8. Possibilitar fazer distribuição de software de forma manual e agendada;
14.9. Suportar modo de instalação silenciosa;
14.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
14.11. Possibilitar fazer a distribuição através de agentes de atualização;
14.12. Utilizar tecnologia multicast para evitar tráfego na rede;
14.13. Possibilitar criar um inventário centralizado de imagens;
14.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
14.15. Suporte a WakeOnLan para deploy de imagens;
14.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
14.17. Suportar modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
14.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
14.19. Possibilitar criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
14.20. Permitir iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
14.21. Permitir baixar atualizações para o computador sem efetuar a instalação
14.22. Permitir o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
14.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
14.24. Permitir selecionar produtos a serem atualizados pela console de gerenciamento;
14.25. Permitir selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

CLÁUSULA XVI – AMBIENTE VIRTUAL

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

A Solução deve possuir as seguintes características mínimas obrigatórias:

15.1.Proteção Sem Agentes

15.1.1. Características mínimas:

15.1.1.1. Capacidade prover proteção das máquinas virtuais de Sistemas Operacionais Windows em hosts VMware ESXi sem a necessidade de instalar agentes (software de proteção) em cada máquina virtual.

15.1.1.2. Capacidade prover proteção das máquinas virtuais de Sistemas Operacionais Windows em hosts VMware ESXi sem a necessidade de instalar agentes em cada máquina virtual.

15.1.1.3. Capacidade de proteger o sistema de arquivos de máquinas virtuais, verificando todos os arquivos abertos e fechados pelo usuário ou por aplicações contra vírus, worms, trojans, adwares, auto-dialers e outras ameaças, baseado em assinatura, usando heurística.

15.1.1.4. Caso o arquivo verificado contenha vírus ou código malicioso, a solução proposta deve desinfectar ou bloquear o acesso ao arquivo.

15.1.1.5. Capacidade de realizar varreduras agendadas e sob demanda no sistema de arquivo das máquinas virtuais.

15.1.1.6. Possuir tecnologia Cloud de verificação de arquivos, em paralelo com as vacinas.

15.1.1.7. Capacidade de proteger o tráfego de máquinas virtuais contra ataques de rede ou exploração de vulnerabilidades (IPS).

15.1.1.8. Capacidade de proteger o tráfego web (HTTP) das máquinas virtuais contra sites e arquivos maliciosos.

15.1.1.9. Capacidade de atualizar as assinaturas de maneira agendada e sob demanda, de maneira incremental.

15.1.1.10. Capacidade de fazer um "rollback" das assinaturas;

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

15.1.1.12. Capacidade de limitar o tamanho máximo de arquivos compactados que serão verificados contra vírus

15.1.1.13. Capacidade de limitar o tempo máximo de varredura de um objeto

15.1.1.14. Possuir gerenciamento central, por onde deve ser possível:

15.1.1.14.1. Instalar a solução de proteção de maneira remota no host ESXi

15.1.1.14.2. Configurar o nível de proteção das máquinas virtuais

15.1.1.14.3. Configurar o nível de proteção das varreduras agendadas e sob demanda.

15.1.1.14.4. Configurar as licenças

15.1.1.14.5. Atualizar as assinaturas de anti-vírus

15.1.1.14.6. Visualizar relatórios de proteção

15.1.1.14.7. Desinstalar a proteção do host VMware ESXi

15.2.Proteção Com Agentes:

15.2.1. Compatibilidade mínima:

15.2.1.1. Arquitetura Virtual:

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

15.2.1.1.1. Windows Server 2008 R2 com a função de Hyper-V instalada
15.2.1.1.2. Windows Server 2008 R2 SP1 com a função de Hyper-V instalada
15.2.1.1.3. Windows Server 2012 com a função de Hyper-V instalada
15.2.1.1.4. Citrix XenServer 6.0.2
15.2.1.1.5. Citrix XenServer 6.1.0

15.2.1.2. Máquinas virtuais
15.2.1.2.1. Windows Vista
15.2.1.2.2. Windows 7
15.2.1.2.3. Windows 8
15.2.1.2.4. Windows 2003 SP2
15.2.1.2.5. Windows 2003 R2
15.2.1.2.6. Windows 2008
15.2.1.2.7. Windows 2008 R2
15.2.1.2.8. Windows 2012
15.2.1.2.9. Windows Small Business Server 2008
15.2.1.2.10. Windows Small Business Server 2011

15.2.2. Características:

15.2.2.1. Toda carga de varredura de arquivos e banco de dados de vacinas de vírus devem ser centralizadas em uma única máquina virtual cliente por host físico. Esta máquina virtual (aqui chamada de SV – Servidor de Varredura) deve ser responsável por verificar os arquivos acessados, criados ou modificados nas outras máquinas virtuais que estão sendo executadas no mesmo host, e responder a elas o veredito (se o arquivo está infectado ou limpo).
15.2.2.2. O SV de ter capacidade de proteger o sistema de arquivos de máquinas virtuais, verificando todos os arquivos abertos e fechados pelo usuário ou por aplicações contra vírus, worms, trojans, adwares, auto-dialers e outras ameaças, baseado em assinatura, usando heurística.
15.2.2.3. Caso o arquivo verificado contenha vírus ou código malicioso, a solução proposta deve desinfectar ou bloquear o acesso ao arquivo.
15.2.2.4. O SV deve ter capacidade de realizar varreduras agendadas e sob demanda no sistema de arquivo das máquinas virtuais.
15.2.2.5. O SV deve possuir tecnologia Cloud de verificação de arquivos, em paralelo com as vacinas.
15.2.2.6. Capacidade de proteger o tráfego de máquinas virtuais contra ataques de rede ou exploração de vulnerabilidades (IPS).
15.2.2.7. Capacidade de proteger o tráfego web (HTTP) das máquinas virtuais contra sites e arquivos maliciosos.
15.2.2.8. O SV deve ter capacidade de atualizar as assinaturas de maneira agendada e sob demanda, de maneira incremental.
15.2.2.9. O SV deve ter capacidade de fazer um "rollback" das assinaturas;
15.2.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independente do nível das ameaças encontradas no período (alta, média ou baixa).
15.2.2.11. O SV deve ter a capacidade de limitar o tamanho máximo de arquivos compactados que serão verificados contra vírus.

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

15.2.2.12. O SV deve ter a capacidade de limitar o tempo máximo de varredura de um objeto

15.2.2.13. Possuir um firewall para cada máquina virtual, com a possibilidade de criação e regras por aplicativo e pacotes de rede.

15.2.2.14. Possuir funcionalidades de controle de inicialização de aplicativo, onde seja possível criar regras especificando quais executáveis ou programas podem ou não ser executados pelo usuário.

15.2.2.15. Possuir funcionalidades de controle de dispositivos, onde seja possível criar regras especificando quais dispositivos podem ser conectados na máquina virtual.

15.2.2.16. Possuir funcionalidades de controle de acesso à web, onde seja possível criar regras especificando quais endereços da web ou tipos de conteúdo podem ser acessados pelos usuários das máquinas virtuais.

15.2.2.17. O gerenciamento central deve permitir:

15.2.2.17.1. Instalar a solução de proteção de maneira remota no host ESXi

15.2.2.17.2. Configurar o nível de proteção das máquinas virtuais

15.2.2.17.3. Configurar o nível de proteção das varreduras agendadas e sob demanda.

15.2.2.17.4. Configurar as licenças

15.2.2.17.5. Atualizar as assinaturas de anti-vírus

15.2.2.17.6. Visualizar relatórios de proteção

15.2.2.17.7. Desinstalar a proteção do host VMware ESXi

15.2.2.17.8. Deve ser gerenciado pela mesma console de gerenciamento dos endpoints.

CLÁUSULA XVI – SUPORTE REMOTO POR PERÍODO DE 12 (*doze*) MESES

16.1. Durante a vigência do contrato deverá ser fornecido suporte técnico pela CONTRATADA seguindo as especificações abaixo:

16.2. Apoio às respostas a incidentes de segurança envolvendo Malware;

16.3. Suporte técnico para eventuais dúvidas ou problemas com a solução;

16.4. Acompanhamento nos chamados escalados para a FABRICANTE em situações de falhas/problemas desconhecidos pelo suporte técnico da CONTRATADA ou bug's;

16.5. O atendimento deverá ser realizado via contato telefônico ou ferramenta de acesso remoto independentemente do tipo de incidente;

16.6. Suporte técnico telefônico fornecido em horário comercial de segunda a sexta feira das 08:00 as 18:00 prestado unicamente à equipe de segurança da área de informática da Prefeitura Municipal de Congonhas, referente a problemas de funcionamento/configuração dos produtos fornecidos;

16.7. Número de chamados ilimitados;

José de Freitas Cardeiro
Prefeito Municipal de Congonhas

16.8. Tempo de atendimento telefônico máximo de duas horas após a abertura do chamado técnico;

16.9. Incidentes, chamados, e problemas escalados ao FABRICANTE deverão ter o acordo de nível de serviço (SLA) abaixo:

16.9.1. **Severidade Nível 1** (Crítico – Onde afeta o serviço prestado do CONTRATANTE por interrupções da solução de antivírus nos sistemas operacionais, possíveis perda de dados, alterações de configuração padrão para configuração insegura e onde não há solução alternativa disponível): 6 horas (Horário Comercial);

16.9.2. **Severidade Nível 2** (Alto – Onde afeta a funcionalidade do produto, mas não causa corrupção e perda de dados ou travamento sistemas): 10 horas (Horário Comercial);

16.9.3. **Severidade Nível 3** (Médio – Solicitações não críticas onde não afeta a funcionalidade do produto): 12 horas (Horário Comercial);

16.9.4. **Severidade Nível 4** (Baixo – Solicitações não críticas ou solicitação de serviços. Todos os incidentes que não satisfaçam um dos critérios listados acima, serão classificados a esse nível de gravidade): 14 horas (Horário Comercial);

16.10. Suporte Técnico

16.10.1. Será exigido da licitante vencedora a comprovação de possuir em seu quadro de funcionários pelo menos 02 técnicos, certificados pelo fabricante do software fornecido, e preparados para dar todo o suporte técnico e ajuda necessária para maximizar os benefícios oferecidos pelo software, aumentando a sua performance, garantindo a melhor estratégia de defesa e minimizando os riscos e impactos de uma tentativa de infecção e/ou invasão. A comprovação de atendimento a este item se dará mediante anexação, na proposta técnica/comercial, das certificações destes técnicos, e também por documento que comprove o vínculo empregatício (*carteira de trabalho ou contrato social*).

CLÁUSULA XVII – ESPECIFICAÇÕES DO SERVIDOR DE ADMINISTRAÇÃO DO SISTEMA DE ANTIVÍRUS

17.1.Especificações mínimas para o servidor de administração de Anti-Vírus:

17.1.1. Requisitos mínimos de hardware

17.1.1.1. Servidor em torre;

17.1.1.2. Processador Intel® Xeon® Quad Core E3-1220 v6, 8GB de memória e HD de 1TB;

17.1.1.3. Intel Xeon E3-1220 v6 de 3 GHz, cache de 8 MB, 4 núcleos/4 segmentos, turbo (72 W);

17.1.1.4. Sem RAID com SATA incorporado;

17.1.1.5. UDIMM DE 8 GB, 2400 MT/S, ECC, BCC;

17.1.1.6. 1TB 7.2K RPM SATA 6Gbps 3.5in Cabled Hard Drive;

17.1.1.7. 5 (cinco) anos de Garantia de reparo básico de hardware: 5 dias na semana e em até 10 horas no local no próximo dia útil, somente para hardware;

de Freitas Cordeiro
Município de Congonhas

17.1.2. Requisitos de Software:

17.1.2.1. Fornecimento de licença do Sistema Operacional Windows Server 2012 R2 Standard Edition.

CLÁUSULA XVIII - DAS OBRIGAÇÕES DA CONTRATADA

18.1. A CONTRATADA obriga-se, além das demais obrigações estabelecidas no edital e seus anexos, à:

18.1.1. Prestar os serviços solicitados, assumindo inteira responsabilidade por estes, por atrasos e/ou defeitos.

18.1.2. Assumir inteira responsabilidade civil, administrativa e penal por quaisquer danos e prejuízos materiais ou pessoais causados pela CONTRATADA, seus empregados ou prepostos, aos CONTRATANTES ou a terceiros.

18.1.3. Responsabilizar-se pelas despesas referentes aos encargos diretos e indiretos, transporte, frete, mão-de-obra, encargos sociais, trabalhistas, previdenciários, securitários e tributários ou outros decorrentes ou que venham a ser devidos em razão da prestação de serviço, obrigando-se a saldá-los na época própria, vez que os seus técnicos não terão vínculo empregatício com os CONTRATANTES, não cabendo a estes quaisquer custos adicionais decorrentes da execução do contrato, que não tenham sido incluídas nos preços propostos.

18.1.4. Manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação devendo comunicar aos CONTRATANTES, imediatamente, qualquer alteração que possa comprometer a manutenção do contrato.

18.1.5. Não ceder ou transferir a terceiros o presente contrato, total ou parcialmente, sem prévia autorização dos CONTRATANTES, por escrito, sob pena de aplicação de sanção, inclusive rescisão.

18.1.6. Substituir ou repor, às suas expensas, imediatamente, no todo ou em parte, o material que apresente vícios, defeitos ou incorreção de qualidade ou quantidade, que o(s) torne(m) impróprio(s) ou inadequado(s) ao fim a que se destina ou lhe(s) diminua o valor, ficando a CONTRATADA responsável por todo e qualquer dano causado aos CONTRATANTES ou a terceiros, em decorrência da paralisação da prestação do serviço.

18.1.7. A CONTRATADA obriga-se ainda a realizar todos os serviços de Assistência Técnica, referente à garantia do funcionamento, utilizando todo o material próprio e necessário, observando todas as normas de segurança e legislação pertinente.

18.1.8. Cumprir rigorosamente com todas as programações e atividades do objeto deste processo licitatório, inclusive com a eventual migração de dados/informações

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

existentes nos sistemas atuais para os sistemas a serem implantados, devendo arcar com os custos de tal operação.

18.1.9. Levar, imediatamente, ao conhecimento do órgão Gestor do Contrato, qualquer fato extraordinário ou anormal que ocorra durante a execução dos serviços, para adoção de medidas cabíveis, bem como, comunicar, por escrito e de forma detalhada.

18.1.10. Apresentar os produtos definidos na qualidade e prazos estabelecidos pelo CONTRATANTE.

18.1.11. Fornecer todas as informações e esclarecimentos solicitados pelo CONTRATANTE. PREFEITURA MUNICIPAL DE CONGONHAS.

18.1.12. Facilitar a supervisão, acompanhamento dos trabalhos pelo CONTRATANTE, fornecendo, sempre que solicitados, informações e documentos relacionados com a execução do objeto do presente edital.

18.1.13. Obedecer às normas e rotinas do CONTRATANTE, principalmente as que disserem respeito à segurança, guarda, manutenção e integridade das informações existentes ou geradas durante a execução dos serviços.

18.1.14. Guardar o mais absoluto sigilo em relação às informações ou documentos de qualquer natureza a que venham tomar conhecimento, respondendo, administrativa, civil e criminalmente por sua indevida divulgação e / ou incorreta ou descuidada utilização.

18.1.15. Responsabilizar-se por todos os ônus referentes aos serviços contratados.

18.1.16. Responsabilizar-se pela conformidade e qualidade dos serviços.

18.1.17. Em nenhuma hipótese veicular publicidade ou qualquer outra informação acerca das atividades, sem prévia autorização do CONTRATANTE.

18.1.18. Fornecer toda e qualquer documentação, projetos, manuais, etc., produzidos durante a execução do objeto do Contrato, de forma convencional e em meio magnético (CD Rom).

18.1.19. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei n° 8.078, de 1990);

18.1.20. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;

18.1.21. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

José de Freitas Cardeiro
Prefeito Municipal de Congonhas

18.1.22. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

18.1.23. Não transferir a outrem, no todo ou em parte, o objeto do presente Termo de Referência, sem prévia e expressa anuência da CONTRATANTE;

18.1.24. Zelar pela perfeita execução dos serviços contratados e atender, de imediato, às solicitações da Contratante, corrigindo nos prazos máximos previstos para atendimento, após a notificação, qualquer ocorrência de interrupção na prestação do(s) serviço(s); devendo, ainda, atender no prazo máximo de 12 (doze) horas a partir da notificação inicial, todas as reincidências e falhas consequentes ao atendimento que as tenha originado;

18.1.25. Em havendo necessidade, aceitar os acréscimos ou supressões nos quantitativos que se fizerem indispensáveis, sempre nas mesmas condições da proposta, na forma do preceituado no art.65, parágrafo 1º, da Lei nº 8.666/93.

18.1.26. Comprovação de ser a licitante revendedora autorizada de produtos de antivírus coorporativo, mediante declaração da fabricante ou por meio de inscrição na seção "Revendedores" do site do fornecedor.

CLÁUSULA XIX - DAS OBRIGAÇÕES DO CONTRATANTE

19.1. São obrigações do CONTRATANTE:

19.1.1. Comunicar a CONTRATADA toda e qualquer ocorrência relacionada com a execução do serviço;

19.1.2. Efetuar o pagamento à CONTRATADA, na forma convencionada neste termo de referência;

19.1.3. Acompanhar e fiscalizar a execução dos serviços, por meio dos servidores designados como Representantes da Administração, nos termos do Art. 67 da Lei 8.666/93, exigindo seu fiel e total cumprimento;

19.1.4. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

19.1.5. Recusar, qualquer serviço prestado fora das especificações estabelecidas neste Termo de Referência;

19.1.6. Proporcionar todas as facilidades necessárias à boa execução dos serviços, inclusive comunicando à CONTRATADA, por escrito e tempestivamente, qualquer mudança de Administração e endereço de cobrança;

19.1.7. Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.

CLÁUSULA XX - GARANTIA

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

20.1. Durante a vigência do contrato a garantia se dará em forma de suporte técnico e seguirá especificações descritas no Termo de Referência que tratarão as respostas a incidentes de segurança bem como o suporte remoto;

20.2. O prazo para a garantia será de 01 (*um*) ano e se iniciará a contar a partir do aceite definitivo do objeto;

20.3. A localização para efeitos de garantia/suporte técnico deverá considerar o seguinte endereço: Prefeitura Municipal de Congonhas, Praça JK s/n, Congonhas-MG, CEP: 36.415-000.

20.4. Incluem-se, na garantia, os serviços de manutenção, suporte técnico, atualização de software e produto, bem como outras despesas decorrentes destes serviços, sem ônus ao CONTRATANTE, salvo quando for provocado por uso inadequado.

CLÁUSULA XXI – CRITÉRIOS DE ACEITABILIDADE E DINÂMICA DE EXECUÇÃO

21.1. O serviço será recebido conforme tipo, qualidade, medidas/dimensões, e demais especificações constantes na Proposta apresentada, acompanhado da respectiva Nota Fiscal. O recebimento da execução do serviço será provisório mediante recibo do funcionário da Diretoria de Tecnologia da Informação, e o recebimento definitivo se dará no prazo de 2 dias úteis do recebimento provisório depois de verificada a qualidade e quantidade por um servidor designado por esta diretoria.

21.2. Após a assinatura do contrato, a Contratada deverá entregar as licenças em até 15 (quinze) dias úteis, contados do recebimento da nota de empenho;

21.3. A CONTRATADA alocará um coordenador de projeto, com capacitação técnica na solução oferecida, que atuará como interface entre a equipe da Prefeitura Municipal de Congonhas e a equipe da CONTRATADA;

21.4. Os softwares bem como suas licenças deverão ser entregues na Diretoria de Informática da Prefeitura Municipal de Congonhas, Avenida Júlia Kubitschek, Nº 230, Sala 307 - 3º Andar, Centro, Congonhas - MG, CEP 36.415-000, no período das 08 às 12h e das 14 às 18h, em dia de expediente.

21.5. Logística de implantação:

21.5.1. Como a Prefeitura de Congonhas não possui sistema de antivírus a CONTRATADA deverá realizar todos os procedimentos de configuração do servidor de antivírus, a ser fornecido pela CONTRATADA, instalação da solução de antivírus em todas as estações de trabalho e ativação das licenças nos novos computadores que foram adquiridos.

21.5.2. A equipe do de informática da Prefeitura Municipal de Congonhas fará o acompanhamento das instalações e atualização da solução nos computadores da sede da Prefeitura Municipal de Congonhas e em todas as secretarias de governo.

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

21.5.3. Após a implantação, a CONTRATADA disponibilizará um técnico especialista para realizar o treinamento da equipe de informática da Prefeitura Municipal de Congonhas, para que os mesmos sejam capazes de instalar, configurar, monitorar, extrair relatórios e identificar, bloquear e prevenir possíveis ameaças.

CLÁUSULA XXII - PREVISÃO ORÇAMENTÁRIA

22.1. A despesa decorrente da contratação correrá à conta das seguintes Dotações Orçamentárias:

Órgão: 11 – Secretaria Municipal de Administração
Unidade: 04 – Diretoria de Tecnologia da Informação
Centro de Custo: 1631 – Informatização das Atividades Administrativas
339039 – Outros Serviços de Terceiros – Pessoa Jurídica

Órgão: 11 – Secretaria Municipal de Administração
Unidade: 04 – Diretoria de Tecnologia da Informação
Centro de Custo: 1631 – Informatização das Atividades Administrativas
339030 – Outros Serviços de Terceiros – Pessoa Jurídica

CLÁUSULA XXIII - DAS SANÇÕES

23.1. Nas hipóteses de inexecução total ou parcial dos serviços ora previstos, de execução de serviço em desacordo com as regras previstas no Termo de Referência ou descumprimento de obrigação, o Município, garantida a prévia defesa, poderá aplicar à CONTRATADA:

a) 0,03%(três centésimos por cento) sobre o valor total do contrato por dia de atraso no início da execução dos serviços, limitados a 10 (dez) dias;

b) 0,1% (um décimo por cento) sobre o valor total do contrato por dia de atraso, limitados a 20 (vinte) dias, por descumprimento das obrigações atinentes à manutenção e obrigações mensais sucessivas, caracterizando, após este prazo, inexecução contratual; Pela inexecução total ou parcial das disposições contratuais, fica sujeita a empresa contratada, garantida a prévia defesa, às penalidades previstas no artigo 87 da Lei 8.666/93, além da aplicação de multa compensatória no valor de 10% (dez) por cento sobre o valor do contrato;

23.2. A inexecução total do contrato nas condições previstas no Termo de Referência e, a critério da Prefeitura Municipal de Congonhas, descumprimento de condições contratuais, reiteradas aplicações de multas ou ainda sistemáticos descumprimentos dos níveis de serviço, sem adoção tempestiva das medidas saneadoras solicitadas pela Prefeitura Municipal de Congonhas, podem ensejar:

a) Rescisão contratual;

b) Sanção de impedimento de licitar e contratar com a Prefeitura Municipal de Congonhas;

c) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

penalidade, que será concedida sempre que o contatado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

23.3. As sanções previstas neste Edital e no Contrato podem ser aplicadas cumulativamente e não têm caráter compensatório. Portanto, não isentam a CONTRATADA da obrigação de indenizar eventuais perdas e danos. Adicionalmente, dependendo da gravidade, a CONTRATADA poderá estarsujeita a outras sanções previstas em Lei.

23.4. A licitante convocada dentro do prazo de validade da sua proposta, que se recusar injustificadamente a prestar os serviços, apresentar pendências junto aos cadastros da Administração Pública, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar a prestação do serviço, deixar de substituir prestação de serviço recusada no prazo previsto, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantido o direito prévio da citação e da ampla defesa, poderá ser impedida de licitar e contratar com a Administração Pública, pelo prazo de até 02 (dois) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, ficando ainda sujeita à multa de 5% (cinco por cento) do valor unitário da proposta, devidamente atualizado, sem prejuízo da aplicação das sanções previstas no neste Edital e das demais cominações legais.

23.5. O contratado deverá manter, durante toda a prestação dos serviços, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação (art. 55, XIII, da Lei nº 8.666/93), sob pena de se lhe aplicar, cumulativamente:

a) Multa no percentual de 20% (vinte por cento) sobre o valor dos serviços constantes da Autorização de Serviços, nos termos do art. 87, II da Lei nº 8.666/93.

b) Rescisão Contratual, nos termos do art. 78, I da Lei 8.666/93.

c) Retenção dos créditos decorrentes do contrato até o limite dos prejuízos causados à Administração, nos termos do art. 80, IV da Lei nº 8.666/93.

CLÁUSULA XXIV – DA RESCISÃO

24.1. A Administração, observadas as razões de conveniência e oportunidade, devidamente justificadas, poderá revogar a qualquer momento o presente procedimento, ou declarar a sua nulidade por motivo de ilegalidade, mediante despacho fundamentado.

24.2. A contratada terá direito à indenização em decorrência da anulação ou revogação deste procedimento licitatório, desde atendidos os requisitos do art.59, parágrafo único da Lei 8666/93.

CLAUSULA XXV - DO PRAZO DE VIGÊNCIA

25.1. A vigência do contrato entre o Município de Congonhas e a vencedora da licitação terá vigência de 12(doze) meses, podendo ser prorrogado por períodos sucessivos de 12(doze)

José de Freitas Cordeiro
Prefeito Municipal de Congonhas

meses, até o máximo de 48 (quarenta e oito) meses desde que ocorra motivo justificado a critério da Administração e interesse das partes.

CLÁUSULA XXVI – GESTÃO DO CONTRATO

26.1. A execução do contrato será gerenciada pela Secretaria Municipal de Administração.

CLÁUSULA XXVII – DA VINCULAÇÃO AO EDITAL

27.1. O presente contrato fica vinculado ao Edital do Processo Licitatório nº. PRC/179/2017, Pregão Presencial nº. PMC/077/2017, Processo Administrativo nº PMC/2206/2017 e ao Termo de Referência, que passam a fazer parte integrante deste contrato, independentemente de transcrição.

CLÁUSULA XXVIII – DO FORO

28.1. Fica eleito o foro da comarca de Congonhas - MG para dirimir dúvidas e decidir pendências jurídicas provenientes deste contrato.

E por estarem as partes justas e contratadas, assinam o presente contrato lavrado em 03 (três) vias de igual teor e forma, juntamente com 02 (duas) testemunhas.

Congonhas, 19 de dezembro de 2017.

José de Freitas Cordeiro
Prefeito Municipal

Luiz Fernando Catizane Soares
Secretário Municipal de Administração

José Glicério Ruas Alves
Microhard Informática Ltda - EPP

TESTEMUNHAS:

1ª

2ª

Diário Oficial Eletrônico
Congonhas - MG
Congonhas, 04 de Janeiro de 2018 – Diário Oficial Eletrônico, criado pela Lei municipal Nº 2.900/2009 – ANO 8 | Nº 1880

CONTRATO DE PRESTAÇÃO DE SERVIÇOS PMC/112/2017

Partes: Município de Congonhas X JTT Locações e Serviços Ltda - ME. Objeto: Prestação de serviços com fornecimento de materiais e mão de obra para manutenção de campos de futebol, no município de Congonhas-MG. O contrato terá vigência de 16 (dezesseis) meses. Valor: R$ 246.500,00. Data: 15/12/2017.

ESTADO DE MINAS GERAIS
MUNICÍPIO DE CONGONHAS

CONTRATO DE PRESTAÇÃO DE SERVIÇOS PMC/113/2017

Partes: Município de Congonhas X Microhard Informática Ltda - EPP. Objeto: Contratação de empresa especializada na prestação de serviços de licenciamento de Antivírus com direito a atualização e suporte técnico para estações de trabalho, servidores de arquivos, incluindo suporte, remoto e/ou in loco e atualização de versão para utilização no parque tecnológico do município de Congonhas-MG e Aquisição de 01 (um) Servidor de Administração do Sistema de Antivírus. O contrato terá vigência de 12 (doze) meses a partir de sua assinatura. Valor: R$ 114.000,00. Data: 19/12/2017.

ESTADO DE MINAS GERAIS
MUNICÍPIO DE CONGONHAS

CONTRATO DE PRESTAÇÃO DE SERVIÇOS PMC/114/2017

Partes: Município de Congonhas X Ortopedia Jaguaribe Indústria e Comércio Ltda. Objeto: O presente contrato tem por objeto aquisição de 02 cadeira de rodas para obeso e 02 cadeira de rodas pediátrica (itens 07 e 08 do Edital do Pregão Eletrônico SRP nº 061/2016), cujos itens constam na Proposta de Aquisição de Equipamentos/Material Permanente do Recurso de Emenda Parlamentar nº27620007 – número da proposta 02566.543000/1160-08 para atender as Clínicas de Especialidades de Saúde do município de Congonhas, conforme descrição dos Itens 7 e 8. O prazo de vigência do contrato será de 12 (doze) meses a partir da data de sua assinatura. Valor: R$5.238,00. Data: 21/12/2017.

ESTADO DE MINAS GERAIS
MUNICÍPIO DE CONGONHAS

CONTRATO DE PRESTAÇÃO DE SERVIÇOS PMC/115/2017

Partes: Município de Congonhas X Ortopedia Jaguaribe Indústria e Comércio Ltda. Objeto: O presente contrato tem por objeto aquisição de 02 cadeira de rodas para obeso e 02 cadeira de rodas pediátrica (itens 07 e 08 do Edital do Pregão Eletrônico SRP nº 061/2016), cujos itens constam na Proposta de Aquisição de Equipamentos/Material Permanente do Recurso de Emenda Parlamentar nº27620007 – número da proposta 02566.543000/1160-08 para atender as Clínicas de Especialidades de Saúde do município de Congonhas, conforme descrição do Item 6. O prazo de vigência do contrato será de 12 (doze) meses a partir da data de sua assinatura. Valor: R$620,00. Data: 21/12/2017.

ESTADO DE MINAS GERAIS
MUNICÍPIO DE CONGONHAS

PRIMEIRO TERMO ADITIVO AO CONTRATO PMC/102/2017

Partes: Município de Congonhas X Trivale Administração Ltda. Objeto: Acréscimo de quantitativos de serviços existentes. Valor: R$807.840,00. Data: 21/12/2017.

ESTADO DE MINAS GERAIS
MUNICÍPIO DE CONGONHAS

QUINTO TERMO ADITIVO AO CONTRATO Nº PMC/001/2013

Partes: Município de Congonhas X Secretaria de Estado de Casa Civil e de Relações Istitucionais-Secri. Objeto: Prorrogação do prazo pelo período de 12 (doze) meses, com início em 31/12/2017 e término em 31/12/2018. Valor: R$199.947,63. Data: 28/12/2017.

ESTADO DE MINAS GERAIS
MUNICÍPIO DE CONGONHAS

CONTRATO DE CREDENCIAMENTO DE SERVIÇOS PMC/111/2017

Partes: Município de Congonhas X Laboratório de Análises Clínicas Ribeiro Carvalho Ltda. Objeto: Credenciamento de Serviços de Exames