| | |
|---|---|
| TERMO DE CONTRATO: | Nº 10/2016 |
| CONTRATANTE: | TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO |
| CONTRATADA: | ESYWORLD SISTEMAS E INFORMÁTICA LTDA. |
| OBJETO DO CONTRATO: | AQUISIÇÃO DE 600 LICENÇAS DE USO, PARA SOLUÇÃO DE ANTIVÍRUS PARA PROTEÇÃO DOS ENDPOINTS DO TCMSP, COM TREINAMENTO E BANCO DE HORAS |
| VIGÊNCIA: | 36 meses |
| DOTAÇÕES: | 10.10.01.032.3024.2100.3390.39 |
| | 77.10.01.032.3014.2009.4490.39 |
| VALOR CONTRATUAL: | R$ 140.000,00 (ESTIMADO) |
| PROCESSO TC: | Nº 72.000.950/16-01 |

O TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO, CNPJ 50.176.270/0001-26, com endereço na Av. Prof. Ascendino Reis 1.130 – São Paulo/SP, neste ato representado por seu Presidente, ROBERTO BRAGUIM, doravante denominado CONTRATANTE, e ESYWORLD SISTEMAS E INFORMÁTICA LTDA., CNPJ 03.899.222/0001-86, com endereço na Rua Newton Prado, 105, São Paulo/SP, doravante denominada CONTRATADA, neste ato representada por seu sócio BINJAMIN HANOCH, RG XXX e CPF XXX, conforme autorização constante do processo TC nº 72.000.950/16-01, resolvem celebrar este contrato, decorrente da licitação na modalidade Pregão nº 07/2016, que se regerá pela legislação sobre licitações e contratos, particularmente a Lei Municipal 13.278/02, Decretos municipais 44.279/03 e 46.662/05 e, no tocante às normas gerais e penais, pelas Leis Federais 8.666/93 e 10.520/02, bem como pelas cláusulas contratuais e condições que seguem:

**CLÁUSULA I) DO OBJETO:** aquisição de 600 Licenças de Uso, para Solução de Antivírus para proteção dos Endpoints; 80 horas técnicas On-site do Fabricante e 6 Vouchers de Treinamento oficial do fabricante, conforme discriminado no Termo de Referência que figura como anexo deste ajuste.

**CLÁUSULA II) DO PREÇO, CONDIÇÕES DE PAGAMENTO E REAJUSTE**

II.1. O valor contratual estimado é de R$ 140.000,00 (cento e quarenta mil reais);

II.1.1. Os preços a serem praticados serão os seguintes:


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

| Descrição | Valor Unit (R$) | Qtde. | Valor Total (R$) |
|---|---|---|---|
| Solução de Antivírus para Proteção dos Endpoints marca/modelo: Kaspersky Endpoint Security for Business – Advanced | 136,00 | 600 licenças | 81.600,00 |
| Horas técnicas On-site do Fabricante (Banco de horas) | 572,50 | 80 horas | 45.800,00 |
| Treinamento Oficial do Fabricante | 2.100,00 | 06 vouchers | 12.600,00 |

II.1.2. Os pagamentos serão feitos através de depósito em conta corrente ou ficha de compensação, ambas de titularidade da CONTRATADA, acompanhado de recibo dos serviços prestados expedido pelo responsável pela fiscalização do instrumento contratual, que necessariamente exerça suas atividades na unidade fiscalizadora dos serviços (Núcleo de Tecnologia da Informação), a ser indicado por autoridade competente, desde que cumpridas todas as exigências legais e contratuais pela CONTRATADA.

II.1.2.1. O pagamento das Licenças e dos Vouchers de Treinamento ocorrerão em até 30 (trinta) dias, contados do recebimento da nota fiscal ou documento equivalente;

II.1.2.2. Os pagamentos dos serviços referentes ao Banco de Horas serão efetuados, no mês subsequente a realização dos serviços, em até 15 (quinze) dias, contados do recebimento da nota fiscal ou documento equivalente.

II.2. O pagamento efetuado com atraso por culpa exclusiva do CONTRATANTE, terão o valor do principal reajustado pelo índice de remuneração básica da caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança para fins de compensação da mora (TR + 0,5% “pro-rata tempore”), observando-se, para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorrer (conforme Portaria 05/2012-SF).

II.3. Na hipótese de erro ou divergência com as condições contratadas, a nota fiscal/fatura será recusada pelo CONTRATANTE mediante declaração expressa das razões da desconformidade, ficando estabelecido que o prazo para pagamento seja contado a partir da data da apresentação da nova fatura devidamente corrigida.

II.4. O preço da Hora técnica On-site do Fabricante (Banco de horas) poderá ser reajustado após um ano da data de apresentação da proposta, limitado à variação do IPC-FIPE ocorrida entre o mês de referência de preços ou o mês do último reajuste aplicado e o mês de aplicação do reajuste ou pelo preço proposto pela CONTRATADA, prevalecendo, para efeito de reajuste, aquele que apresentar menor valor, ou por outro índice estabelecido por superveniência de normas federais e municipais.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

**CLÁUSULA III) DA VIGÊNCIA:** O contrato terá início de vigência a partir da data de sua assinatura e término na data da lavratura do termo de recebimento definitivo.

III.1. O prazo para disponibilização dos downloads das Licenças de Uso é de até 20 (vinte) dias, contados da data fixada na Ordem de Início de Fornecimento;

III.2. O prazo para a entrega dos Vouchers de Treinamento é de até 30 (trinta) dias, contados da data fixada na Ordem de Início de Fornecimento;

III.3. O prazo para suporte técnico é de 36 (trinta e seis) meses contados da data de emissão do Termo de Recebimento Provisório das Licenças de Uso;

III.4. O prazo para utilização do Banco de Horas é de 36 (trinta e seis) meses, contados da data de emissão do Termo de Recebimento Provisório das Licenças de Uso.

**CLÁUSULA IV) DOS RECURSOS ORÇAMENTÁRIOS:** As despesas resultantes deste instrumento correrão por conta dos recursos constantes das dotações orçamentárias 10.10.01.032.3024.2100.3390.39 – Outros Serviços de Terceiros – Pessoa Jurídica, 77.10.01.032.3014.2009.4490.39 – Outros Serviços de Terceiros – Pessoa Jurídica e no próximo exercício, à conta da dotação orçamentária prevista para atender despesas da mesma natureza.

**CLÁUSULA V) DOS DIREITOS E RESPONSABILIDADES DA CONTRATADA:**

V.1. Executar o objeto deste contrato obedecendo às especificações constantes no Termo de Referência e nas cláusulas deste contrato;

V.2. Manter o mais completo e absoluto sigilo sobre quaisquer dados, informações, documentos, especificações técnicas ou comerciais da CONTRATANTE, dos quais venha a ter conhecimento ou acesso, ou mesmo, venham a lhe ser confiados em razão desta contratação, não podendo, sob qualquer pretexto, reproduzir, utilizar ou deles dar conhecimento a terceiros estranhos à presente contratação sob as penas da Lei, mesmo após a rescisão deste Contrato;

V.3. Ser responsável por eventuais danos causados aos equipamentos e a outros bens de propriedade do CONTRATANTE durante a execução de serviços;

V.4. Responsabilizar-se por todos os tributos e encargos previstos na legislação vigente, inclusive trabalhistas, decorrentes do objeto contratado, obrigando-se a saldá-los na época própria;

V.5. Manter atualizadas, durante a vigência da contratação, todas as condições de habilitação e qualificação exigidas para esta contratação.

**CLÁUSULA VI) DOS DIREITOS E RESPONSABILIDADES DO CONTRATANTE:**

VI.1. Caberá ao responsável pela fiscalização do contrato, necessariamente exercente de funções na unidade fiscalizadora dos serviços (Núcleo de

Tecnologia da Informação), a ser indicado por autoridade competente, na forma do artigo 67 da Lei Federal 8.666/93:

VI.1.1. Expedir a Ordem para Início de Fornecimento, com início de vigência a critério do CONTRATANTE;

VI.1.2. Acompanhar e supervisionar a realização dos serviços pelos técnicos da CONTRATADA;

VI.1.3. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da CONTRATADA;

VI.1.4. Exigir, a qualquer tempo, a comprovação das condições da CONTRATADA que ensejaram sua contratação, notadamente no tocante à qualificação técnica;

VI.1.5. Propor à autoridade competente a aplicação de penalidades, mediante caracterização da infração imputada à **CONTRATADA**, como disposto no art. 54 do Decreto Municipal nº 44.279/03.

VI.1.6. Propor à autoridade competente a dispensa de aplicação de penalidades à **CONTRATADA**, como disposto no art. 56 do Decreto Municipal nº 44.279/03.

VI.1.7. Receber provisoriamente as licenças, após verificada as plenas condições de funcionamento (configuração e implementação), incluindo a transferência de conhecimento para os técnicos do CONTRATANTE, atestando a conformidade do fornecimento e dos serviços executados, em especial quanto ao cumprimento dos prazos e qualidade da execução.

VI.1.8. Receber definitivamente o objeto, mediante termo circunstanciado, após o decurso do prazo de observação ou vistoria que comprove a adequação do objeto aos termos contratuais, observado o disposto no artigo 69 da Lei Federal 8.666/93.

**CLÁUSULA VII) DA RESCISÃO:** Este contrato poderá ser rescindido, independentemente de interpelação judicial ou extrajudicial, nas hipóteses previstas na Lei Municipal 13.278/02 e Decretos Municipais 44.279/03 e 46.662/05 e na Lei Federal 8.666/93.

**CLÁUSULA VIII) DAS PENALIDADES:**

VIII.1. O descumprimento das obrigações previstas em lei ou neste contrato sujeitará a CONTRATADA às seguintes multas, que poderão ser aplicadas em conjunto com as demais sanções dispostas na Seção II, do Capítulo IV, da Lei Federal 8.666/93 e art. 7º da Lei Federal 10.520/02.

VIII.1.1. Multa de 1% (um por cento) por dia de atraso no fornecimento do objeto, limitado a 10 (dez) dias úteis, após o que o fornecimento será considerado como definitivamente não realizado, implicando multa de 20% (vinte por cento), ambas calculadas sobre o valor da parcela inadimplida;

VIII.1.2. Multa de 1% (um por cento) por hora, constatado o atraso para atendimento quando de Alta Severidade (Conforme Termo de Referência), limitado a 10 (dez) dias úteis, calculada sobre o valor total do ajuste.

VIII.1.2.1. Em caso de reincidência, o percentual acima referido poderá ser majorado para 1,5% (um inteiro e cinco décimos por cento).

VIII.1.3. Multa de 0,5% (cinco décimos por cento) por hora, constatado o atraso para atendimento quando de Média/Alta Severidade (Conforme Termo de Referência), limitado a 10 (dez) dias úteis, calculada sobre o valor total do ajuste.

VIII.1.4. Multa de 0,5% (cinco décimos por cento) por dia, constatado o atraso para atendimento quando de Baixa Severidade (Conforme Termo de Referência), limitada a 10 (dez) dias úteis, calculada sobre o valor total do ajuste.

VIII.1.5. Multa de 1% (um por cento) por dia, constatado o descumprimento de obrigações relacionadas no Termo de Referência que figura como anexo deste ajuste, excetuando-se as situações onde foram estabelecidas multas específicas, ou seja, as três subcláusulas anteriores, limitada a 10 (dez) dias, calculada sobre o valor total do ajuste.

VIII.1.6. Multa de 5% (cinco por cento) do valor total deste instrumento, caso a CONTRATADA dê causa à rescisão do ajuste sem motivo justificado e aceito pelo CONTRATANTE.

VIII.2. As multas são independentes, ou seja, a aplicação de uma não exclui a das outras, devendo ser recolhidas ou descontadas de pagamentos eventualmente devidos pelo CONTRATANTE em até 5 (cinco) dias úteis contados a partir de sua comunicação à CONTRATADA ou, ainda, se for o caso, cobradas judicialmente.

VIII.2.1. O não recolhimento das multas no prazo implicará atualização monetária e juros moratórios calculados em conformidade com a Lei Municipal 13.275/2002.

VIII.3. No caso de aplicação de eventuais penalidades, será observado o procedimento previsto no Capítulo X do Decreto Municipal nº 44.279/03 e na Seção II do Capítulo 4 da Lei Federal nº 8.666/93.

**CLÁUSULA IX) DA ANTICORRUPÇÃO**: Para a execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma a ele não relacionada, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma, conforme disposto no Decreto Municipal n° 56.633/2015.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

**CLÁUSULA X) LEGISLAÇÃO APLICÁVEL:** Leis Federais 8.666/93 e 10.520/02, Lei Municipal 13.278/02, Decretos municipais 44.279/03 e 46.662/05 e legislação correlata, cabendo ao CONTRATANTE decidir sobre os casos omissos.

**CLÁUSULA XI) DA TAXA DE SERVIÇOS RELATIVA À LAVRATURA DO CONTRATO**: Recolhe-se, neste ato, o preço público relativo à prestação de serviços administrativos no valor de R$ 79,00 (setenta e nove reais).

**CLÁUSULA XII) DA DOCUMENTAÇÃO INTEGRANTE DO CONTRATO:** São partes integrantes deste contrato o edital do Pregão 07/2016 e seus anexos, bem como a proposta da CONTRATADA.

**CLÁUSULA XIII) DO FORO:** Fica eleito o Foro da Comarca desta Capital para solução de quaisquer litígios relativos ao presente ajuste, com renúncia expressa de qualquer outro por mais privilegiado que seja.

E, por estarem de acordo, as partes firmam o presente, em duas vias de igual teor.

São Paulo, 15 de junho de 2016.

**ROBERTO BRAGUIM**
Presidente
**TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO**

**BINJAMIN HANOCH**
Sócio
**ESYWORLD SISTEMAS E INFORMÁTICA LTDA.**


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

## ANEXO I – TERMO DE REFERÊNCIA

## ESPECIFICAÇÕES TÉCNICAS

### I - OBJETO

Aquisição de Licenças de Uso de Solução de Antivírus para os Endpoints do TCMSP, com Treinamento e Banco de Horas.

### II - PRODUTOS

| Item | Qtde. | Descrição do Produto |
|---|---|---|
| 01 | 600 Licenças | Solução de Antivírus para Proteção dos Endpoints |
| 02 | 80 Horas | Horas técnicas On-site do Fabricante |
| 03 | 6 Vouchers | Treinamento Oficial do Fabricante |

### III - DISCRIMINAÇÃO GERAL

Todas as funcionalidades solicitadas deverão ser atendidas por uma única solução/produto, não sendo aceitas composições de soluções;

As Licenças deverão ser fornecidas através de Download;

A Licitante deverá apresentar uma carta do Fabricante, informando o grau de parceria;

Declaração do fabricante, comprovando que a Licitante está autorizada a comercializar o produto objeto desta licitação ou, alternativamente, a declaração do fabricante poderá ser substituída por cópia de “home page” do referido fabricante no Brasil, comprovando que a Licitante é revenda autorizada;

Os preços cotados do objeto da presente licitação deverão ser expressos em moeda corrente nacional, neles inclusos os acréscimos e despesas, como impostos, sem inclusão de qualquer encargo financeiro ou previsão inflacionária, sem que sofra correção ou reajuste durante o período licitatório.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

## IV – ESPECIFICAÇÕES TÉCNICAS

1. Servidor de Administração e Console Administrativa

1.1. Compatibilidade:

1.1.1. Microsoft Windows 10 Pro x86 / x64.
1.1.2. Microsoft Windows 10 Enterprise x86 / x64.
1.1.3. Microsoft Windows 8.1 Pro x86 / x64.
1.1.4. Microsoft Windows 8.1 Enterprise x86 / x64.
1.1.5. Microsoft Windows 8 Pro x86 / x64.
1.1.6. Microsoft Windows 8 Enterprise x86 / x64.
1.1.7. Microsoft Windows 7 Professional x86 / x64 SP1 and later.
1.1.8. Microsoft Windows 7 Enterprise / Ultimate x86 / x64 SP1 and later.
1.1.9. Microsoft Windows 7 Professional x86 / x64.
1.1.10. Microsoft Windows 7 Enterprise / Ultimate x86 / x64.
1.1.11. Microsoft Windows Vista x86 / x64 SP2 and later.
1.1.12. Microsoft Windows XP Professional x86 SP3 and later.
1.1.13. Microsoft Windows Server 2012 R2 Standard / Essentials / Enterprise x64 (ReFS file system is supported with limitations, Server Core and Cluster Mode configurations are not supported).
1.1.14. Microsoft Windows Server 2012 Foundation / Standard / Essentials x64 (ReFS file system is supported with limitations, Server Core and Cluster Mode configurations are not supported).
1.1.15. Microsoft Small Business Server 2011 Standard / Essentials x64.
1.1.16. Microsoft Windows MultiPoint Server 2011 x64.
1.1.17. Microsoft Windows Server 2008 R2 Standard / Enterprise / Foundation x64 SP1 and later.
1.1.18. Microsoft Windows Server 2008 R2 Standard / Enterprise / Foundation x64.
1.1.19. Microsoft Windows Server 2008 Standard / Enterprise x86 / x64 SP2 and later.
1.1.20. Microsoft Small Business Server 2008 Standard / Premium x64.
1.1.21. Microsoft Windows Server 2003 R2 Standard / Enterprise x86 / x64 SP2 and later.
1.1.22. Microsoft Windows Server 2003 Standard / Enterprise x86 / x64 SP2 and later.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

1.1.23. Microsoft Windows Embedded 8.0 Standard x64.

1.1.24. Microsoft Windows Embedded 8.1 Industry Pro x64.

1.1.25. Microsoft Windows Embedded Standard 7* x86 / x64 SP1.

1.1.26. Microsoft Windows Embedded POSReady 7* x86 / x64.

1.2. Suporta as seguintes plataformas virtuais:

1.2.1. Microsoft Windows Server 2008 R2 SP1 - Função Hyper-V (no modo de instalação completa) com todas as atualizações disponíveis instaladas.

1.2.2. Microsoft Windows Server 2012 - Função Hyper-V (no modo de instalação completa) com todas as atualizações disponíveis instaladas.

1.2.3. Microsoft Windows Server 2012 R2 - Função Hyper-V (no modo de instalação completa) com todas as atualizações disponíveis instaladas.

1.2.4. Citrix XenServer 6.1 com todas as correções recomendadas instaladas.

1.2.5. Citrix XenServer 6.2 SP1.

1.2.6. Citrix XenServer 6.5.

1.2.7. VMware ESXi 5.1 com as últimas atualizações instaladas.

1.2.8. VMware ESXi 5.5 com as últimas atualizações instaladas.

1.2.9. VMware ESXi 6.

1.3. Características:

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

1.3.2. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.

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

1.3.4. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets:

1.3.4.1. Android OS 2.3 – 5.1.

1.3.4.2. Apple iOS 7.0 – 8.x.

1.3.4.3. Windows Phone 8.1.

1.3.5. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema Ios.

1.3.6. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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

1.3.8. Capacidade de gerenciar smartphones e tablets:

1.3.8.1. Android OS 2.3 – 5.1.

1.3.8.2. Apple iOS 7.0 – 8.x.

1.3.8.3. Windows Phone 8.1.

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

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

1.3.11. 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.

1.3.12. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

1.3.13. Capacidade de aplicar atualizações do Windows remotamente nas estações e servidores.

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

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

1.3.16. 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.

1.3.17. 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.

1.3.18. 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.

1.3.19. 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.

1.3.20. Deve fornecer as seguintes informações dos computadores:

1.3.20.1. Se o antivírus está instalado.

1.3.20.2. Se o antivírus está iniciado.

1.3.20.3. Se o antivírus está atualizado.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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

1.3.20.5. Minutos/horas desde a última atualização de vacinas.

1.3.20.6. Data e horário da última verificação executada na máquina.

1.3.20.7. Versão do antivírus instalado na máquina.

1.3.20.8. Se é necessário reiniciar o computador para aplicar mudanças.

1.3.20.9. Data e horário de quando a máquina foi ligada.

1.3.20.10. Quantidade de vírus encontrados (contador) na máquina.

1.3.20.11. Nome do computador.

1.3.20.12. Domínio ou grupo de trabalho do computador.

1.3.20.13. Data e horário da última atualização de vacinas.

1.3.20.14. Sistema operacional com Service Pack.

1.3.20.15. Quantidade de processadores.

1.3.20.16. Quantidade de memória RAM.

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

1.3.20.18. Endereço IP.

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

1.3.20.20. Atualizações do Windows Updates instaladas.

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

1.3.20.22. Vulnerabilidades de aplicativos instalados na máquina.

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

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

1.3.22.1. Mudança de gateway.

1.3.22.2. Mudança de subnet DNS.

1.3.22.3. Mudança de domínio.

1.3.22.4. Mudança de servidor DHCP.

1.3.22.5. Mudança de servidor DNS.

1.3.22.6. Mudança de servidor WINS.

1.3.22.7. Aparecimento de nova subnet.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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

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

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

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

1.3.27. 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.

1.3.28. 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.

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

1.3.30. Capacidade de gerar traps SNMP para monitoramento de eventos.

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

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

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

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

1.3.35. 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.

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

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

1.3.38. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

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


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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

1.3.41. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2. Estações Windows

2.1. Compatibilidade:

2.1.1. Microsoft Windows XP Professional SP3 e superior.

2.1.2. Microsoft Windows Vista Business/Enterprise/Ultimate SP2.

2.1.3. Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2.

2.1.4. Microsoft Windows 7 Professional/Enterprise/Ultimate.

2.1.5. Microsoft Windows 7 Professional/Enterprise/Ultimate x64.

2.1.6. Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 e superior.

2.1.7. Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1 e superior.

2.1.8. Microsoft Windows 8 Professional/Enterprise.

2.1.9. Microsoft Windows 8 Professional/Enterprise x64.

2.1.10. Microsoft Windows 8.1 Professional/Enterprise.

2.1.11. Microsoft Windows 8.1 Professional/Enterprise 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. Firewall com IDS.

2.2.1.6. Autoproteção (contra ataques aos serviços/processos do antivírus).

2.2.1.7. Controle de dispositivos externos.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

2.2.1.8. Controle de acesso a sites por categoria.

2.2.1.9. Controle de execução de aplicativos.

2.2.1.10. Controle de vulnerabilidades do Windows e dos aplicativos instalados, utilizando a mesma console do Antivírus.

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

2.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas 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 automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução.

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

2.2.6. 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.

2.2.7. 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.

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

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

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

2.2.11. Capacidade de verificar somente arquivos novos e alterados.

2.2.12. Capacidade de verificar objetos usando heurística.

2.2.13. Capacidade de agendar uma pausa na verificação.

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:


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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 verificação de corpo e anexos de e-mails usando heurística.

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

2.2.21.1. Perguntar o que fazer, ou;

2.2.21.2. Bloquear o e-mail:

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

2.2.21.2.2. Caso positivo de desinfecção:

2.2.21.2.2.1. Restaurar o e-mail para o usuário.

2.2.21.2.3. Caso negativo de desinfecção:

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

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

2.2.23. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

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

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

2.2.26. Deve ter suporte total ao protocolo IPv6.

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


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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

2.2.28.1. Perguntar o que fazer, ou;

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

2.2.28.3. Permitir acesso ao objeto.

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

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

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

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

2.2.31. 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.

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

2.2.33. 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.

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

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

2.2.36. 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.

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

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

2.2.37.2. 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.

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

2.2.38.1. Discos de armazenamento locais.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

2.2.38.2. Armazenamento removível.

2.2.38.3. Impressoras.

2.2.38.4. CD/DVD.

2.2.38.5. Drives de disquete.

2.2.38.6. Modems.

2.2.38.7. Dispositivos de fita.

2.2.38.8. Dispositivos multifuncionais.

2.2.38.9. Leitores de smart card.

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

2.2.38.11. Wi-Fi.

2.2.38.12. Adaptadores de rede externos.

2.2.38.13. Dispositivos MP3 ou smartphones.

2.2.38.14. Dispositivos Bluetooth.

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

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

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

2.2.42. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

2.2.43. 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.

2.2.44. 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).

2.2.45. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

2.2.46. 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.

2.2.47. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso a web.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

2.2.48. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso a web.

3. Estações e Servidores Mac OS X

3.1. Compatibilidade:

3.1.1. Mac OS X 10.11 (El Capitan).

3.1.2. Mac OS X 10.10 (Yosemite).

3.1.3. Mac OS X 10.9 (Mavericks).

3.1.4. Mac OS X 10.8 (Mountain Lion).

3.1.5. Mac OS X 10.7 (Lion).

3.1.6. Mac OS X 10.6 (Snow Leopard).

3.1.7. Mac OS X 10.5 (Leopard).

3.1.8. Mac OS X 10.4 (Tiger).

3.1.9. Mac OS X Server 10.6 (32/64-bit).

3.1.10. Mac OS X Server 10.7 (32/64-bit).

3.2. Características:

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

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

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

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

3.2.5. Capacidade de voltar para a base de dados de vacina anterior.

3.2.6. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

3.2.7. Deve permitir, por meio da console da ferramenta, extrair um artefato em quarentena de um cliente.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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

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

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

3.2.11. Capacidade de verificar somente arquivos novos e alterados.

3.2.12. Capacidade de verificar objetos usando heurística.

3.2.13. Capacidade de agendar uma pausa na verificação.

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

3.2.14.1. Perguntar o que fazer, ou;

3.2.14.2. Bloquear acesso ao objeto:

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

3.2.14.2.2. Caso positivo de desinfecção:

3.2.14.2.2.1. Restaurar o objeto para uso.

3.2.14.2.3. Caso negativo de desinfecção:

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

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

3.2.16. Capacidade de verificar arquivos de formato de e-mail.

3.2.17. 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.

3.2.18. 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:


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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 32-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.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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 tomá-la 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:

5.1.1. Microsoft Windows 10 Pro x86 / x64.

5.1.2. Microsoft Windows 10 Enterprise x86 / x64.

5.1.3. Microsoft Windows 8.1 Pro x86 / x64.

5.1.4. Microsoft Windows 8.1 Enterprise x86 / x64.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

5.1.5. Microsoft Windows 8 Pro x86 / x64.

5.1.6. Microsoft Windows 8 Enterprise x86 / x64.

5.1.7. Microsoft Windows 7 Professional x86 / x64 SP1 and later.

5.1.8. Microsoft Windows 7 Enterprise / Ultimate x86 / x64 SP1 and later.

5.1.9. Microsoft Windows 7 Professional x86 / x64.

5.1.10. Microsoft Windows 7 Enterprise / Ultimate x86 / x64.

5.1.11. Microsoft Windows Vista x86 / x64 SP2 and later.

5.1.12. Microsoft Windows XP Professional x86 SP3 and later.

5.1.13. Microsoft Windows Server 2012 R2 Standard / Essentials / Enterprise x64 (ReFS file system is supported with limitations, Server Core and Cluster Mode configurations are not supported).

5.1.14. Microsoft Windows Server 2012 Foundation / Standard / Essentials x64 (ReFS file system is supported with limitations, Server Core and Cluster Mode configurations are not supported).

5.1.15. Microsoft Small Business Server 2011 Standard / Essentials x64.

5.1.16. Microsoft Windows MultiPoint Server 2011 x64.

5.1.17. Microsoft Windows Server 2008 R2 Standard / Enterprise / Foundation x64 SP1 and later.

5.1.18. Microsoft Windows Server 2008 R2 Standard / Enterprise / Foundation x64.

5.1.19. Microsoft Windows Server 2008 Standard / Enterprise x86 / x64 SP2 and later.

5.1.20. Microsoft Small Business Server 2008 Standard / Premium x64.

5.1.21. Microsoft Windows Server 2003 R2 Standard / Enterprise x86 / x64 SP2 and later.

5.1.22. Microsoft Windows Server 2003 Standard / Enterprise x86 / x64 SP2 and later.

5.1.23. Microsoft Windows Embedded 8.0 Standard x64.

5.1.24. Microsoft Windows Embedded 8.1 Industry Pro x64.

5.1.25. Microsoft Windows Embedded Standard 7* x86 / x64 SP1.

5.1.26. Microsoft Windows Embedded POSReady 7* x86 / x64.

5.2. Características:

5.2.1. Deve prover as seguintes proteções:

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


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

5.2.1.2. Autoproteção contra ataques aos serviços/processos do antivírus.

5.2.1.3. Firewall com IDS.

5.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

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

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

5.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

5.2.4.3. Leitura de configurações.

5.2.4.4. Modificação de configurações.

5.2.4.5. Gerenciamento de Backup e Quarentena.

5.2.4.6. Visualização de relatórios.

5.2.4.7. Gerenciamento de relatórios.

5.2.4.8. Gerenciamento de chaves de licença.

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

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

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

5.2.5.2. 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.

5.2.6. 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.

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

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

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


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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

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

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

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

5.2.14. 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.

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

5.2.16. 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 tomá-la a partir da extensão do arquivo.

5.2.17. Capacidade de verificar somente arquivos novos e alterados.

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

5.2.19. Capacidade de verificar objetos usando heurística.

5.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

5.2.21. Capacidade de agendar uma pausa na verificação.

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

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

5.2.23.1. Perguntar o que fazer, ou;

5.2.23.2. Bloquear acesso ao objeto:

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

5.2.23.2.2. Caso positivo de desinfecção:

5.2.23.2.2.1. Restaurar o objeto para uso.

5.2.23.2.3. Caso negativo de desinfecção:

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


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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

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

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

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

6. Servidores Linux

6.1. Compatibilidade:

6.1.1. Plataforma 32-bits:

6.1.1.1. Canaima 3.

6.1.1.2. Red Flag Desktop 6.0 SP2.

6.1.1.3. Red Hat Enterprise Linux 5.8 Desktop.

6.1.1.4. Red Hat Enterprise Linux 6.2 Desktop.

6.1.1.5. Fedora 16.

6.1.1.6. CentOS-6.2.

6.1.1.7. SUSE Linux Enterprise Desktop 10 SP4.

6.1.1.8. SUSE Linux Enterprise Desktop 11 SP2.

6.1.1.9. openSUSE Linux 12.1.

6.1.1.10. openSUSE Linux 12.2.

6.1.1.11. Debian GNU/Linux 6.0.5.

6.1.1.12. Mandriva Linux 2011.

6.1.1.13. Ubuntu 10.04 LTS.

6.1.1.14. Ubuntu 12.04 LTS.

6.1.2. Plataforma 32-bits:

6.1.2.1. Canaima 3.

6.1.2.2. Red Flag Desktop 6.0 SP2.

6.1.2.3. Red Hat Enterprise Linux 5.8.

6.1.2.4. Red Hat Enterprise Linux 6.2 Desktop.

6.1.2.5. Fedora 16.

6.1.2.6. CentOS-6.2.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

6.1.2.7. SUSE Linux Enterprise Desktop 10 SP4.

6.1.2.8. SUSE Linux Enterprise Desktop 11 SP2.

6.1.2.9. OpenSUSE Linux 12.1.

6.1.2.10. openSUSE Linux 12.2.

6.1.2.11. Debian GNU/Linux 6.0.5.

6.1.2.12. Ubuntu 10.04 LTS.

6.1.2.13. Ubuntu 12.04 LTS.

6.1. Características:

6.1.1. Deve prover as seguintes proteções:

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

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

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

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

6.1.2.2. 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.

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

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

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

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

6.1.5. 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 tomá-la a partir da extensão do arquivo.

6.1.6. Capacidade de verificar objetos usando heurística.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

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

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

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

7. Smartphones e tablets

7.1. Compatibilidade:

7.1.1.1. Android OS 2.3 – 5.1.

7.1.1.2. Apple iOS 7.0 – 8.x.

7.1.1.3. Windows Phone 8.1.

7.2. Características:

7.2.1. Deve prover as seguintes proteções para smartphone Android:

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

7.2.1.1.1. Todos os objetos transmitidos usando conexões wireless (porta de infra-vermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.

7.2.1.1.2. Arquivos abertos no smartphone.

7.2.1.1.3. Programas instalados usando a interface do smartphone.

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

7.2.2. Deverá isolar em área de quarentena os arquivos infectados.

7.2.3. Deverá atualizar as bases de vacinas de modo agendado.

7.2.4. Deverá bloquear spams de SMS através de Black lists.

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

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

7.2.7. Deverá ter firewall pessoal.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

7.2.8. Capacidade de bloquear o dispositivo quando um Jailbreak é detectado através de relatórios.

7.2.9. Capacidade de detectar Jailbreak em dispositivos iOS e Android.

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

7.2.11. Capacidade de bloquear o acesso a sites phishing ou malicioso.

7.2.12. Capacidade de criar conteiners de aplicativos, separando dados corporativos de dados pessoais.

7.2.13. Capacidade de configurar White e black list de aplicativos.

8. Gerenciamento de dispositivos móveis (MDM):

8.1. Compatibilidade:

8.1.1. Dispositivos conectados através do Microsoft Exchange ActiveSync:

8.1.1.1. Apple iOS.

8.1.1.2. Windows Phone.

8.1.1.3. Android

8.2. Características:

8.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

8.2.2. Capacidade de ajustar as configurações de:

8.2.2.1. Sincronização de e-mail.

8.2.2.2. Uso de aplicativos.

8.2.2.3. Senha do usuário.

8.2.2.4. Criptografia de dados.

8.2.2.5. Conexão de mídia removível.

8.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

8.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

8.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

8.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS.

8.2.7. Capacidade de instalar e desinstalar aplicativos no iOS/Android remotamente.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

9. Criptografia:

9.1. Compatibilidade:

9.1.1. Microsoft Windows XP Professional SP3 ou superior.

9.1.2. Microsoft Windows Vista Business/Enterprise/Ultimate SP2.

9.1.3. Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2.

9.1.4. Microsoft Windows 7 Professional/Enterprise/Ultimate.

9.1.5. Microsoft Windows 7 Professional/Enterprise/Ultimate x64.

9.1.6. Microsoft Windows 8 Professional/Enterprise.

9.1.7. Microsoft Windows 8 Professional/Enterprise x64.

9.1.8. Microsoft Windows 8.1 Professional / Enterprise.

9.1.9. Microsoft Windows 8.1 Professional / Enterprise x64.

9.2. Características:

9.2.1. Capacidade de gerenciamento em uma console unificada com a ferramenta de antivírus.

9.2.2. 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.

9.2.3. Utilizar, no mínimo, algoritmo AES com chave de 256 bits.

9.2.4. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário.

9.2.5. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot.

9.2.6. Permitir criar vários usuários de autenticação pré-boot.

9.2.7. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento.

9.2.8. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

9.2.8.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes.

9.2.8.2. Criptografar todos os arquivos individualmente.

9.2.8.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas.

9.2.8.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

9.2.9. 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.

9.2.10. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados.

9.2.11. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados.

9.2.12. Verifica compatibilidade de hardware antes de aplicar a criptografia.

10. Gerenciamento de Sistemas:

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

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

10.3. 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.

10.4. Possuir tecnologia de Controle de Admissão de Rede (NAC), com a possibilidade de criar regras de quais tipos de dispositivos podem ter acessos a recursos da rede.

10.5. Capacidade de gerenciar licenças de softwares de terceiros.

10.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas.

10.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros.

## V - SUPORTE

O suporte técnico deverá ser de 36 (trinta e seis) meses, e será acionado em caso de qualquer indisponibilidade da solução, devendo ter como objetivos de atendimento, pelo FABRICANTE, os índices de criticidade a seguir:


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

| ***Criticidade*** | ***Descrição*** | ***Atendimento*** | ***Resolução do Problema*** |
|---|---|---|---|
| Severidade 1 (Alta) | Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema, ou dos dados. Exemplo: Serviço inativo. | 2 a 4 horas | Menos de 5 horas |
| Severidade 2 (Média/Alta) | Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade. a curto prazo, possa ser afetada negativamente. Exemplo: Servidor não responde a comandos ou responde com resultados inesperados. Arquivos de *log* corrompidos ou inexistentes. | 4 a 6 horas | Menos de 10 horas |
| Severidade 3 (Baixa) | Demais problemas que não afetem diretamente o ambiente de produção. Exemplo: Problemas na geração de relatórios e dúvidas gerais de operação/configuração. | 8 a 10 horas | Menos de 30 horas |

Deve possibilitar a abertura de chamados de suporte, para no mínimo, os seguintes métodos: via telefone, via e-mail e via website do fabricante;


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

Todos os prazos para atendimento começarão a ser contados a partir da abertura do chamado, independentemente deste ter sido feito via telefone, via e-mail, ou via Website do fabricante;

Considera-se plenamente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa;

Durante o período de vigência do contrato o fornecedor executará, sem ônus adicionais, correções de falhas (bugs) dos softwares suportados;

Durante o período de vigência do contrato o CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos softwares que fazem parte da solução ofertada;

Canais de Atendimento:

- Será disponibilizado canal de atendimento e chamado técnico em horário comercial, 5 (cinco) dias por semana, através de site na Internet e/ou canal telefônico.

## VI – BANCO DE HORAS

A CONTRATANTE poderá solicitar manutenção corretiva, quando da necessidade de aprimoramento da solução, ou adequação de novos versionamentos, sendo que a quantidade de horas utilizadas será prévia e formalmente ajustadas entre o TCMSP e a CONTRATADA, e serão utilizadas as horas previstas abaixo, as quais serão faturadas pela CONTRATADA, no mês seguinte à sua efetiva utilização:

- 80 (oitenta) horas técnicas a serem prestadas em horário comercial, de segunda a sexta-feira.

O atendimento deverá ser feito presencialmente ou remotamente (dependendo da situação);

Através do aceite, o Fabricante está autorizado a acessar e controlar os computadores ou dispositivos para prover o serviço ao Tribunal;

Os serviços podem não ficar disponíveis por motivos de manutenção ou problemas de internet.

## VII – TREINAMENTOS

Os treinamentos consistirão na capacitação de técnicos do Tribunal nos processos de trabalho, métodos, técnicas e ferramentas integrantes da solução implantada;

O treinamento deverá ser executado por um técnico credenciado e certificado pelo Fabricante;


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632

Deverá ter duração de 16 (dezesseis) horas, sendo 8 (oito) horas por dia;

O mesmo deverá ser realizado, dentro da região metropolitana de São Paulo;

Deverá ser emitido um certificado para cada participante do treinamento;

Os Vouchers de Treinamento deverão ter validade de, no mínimo, 12 meses.


Avenida Prof. Ascendino Reis, 1.130 – CEP 04027-000 – São Paulo
TEL. PABX (11) 5080-1000 – FAX (11) 5572-9632