

CONTRATO DE AQUISIÇÃO

CONTRATO Nº 005/2018

CONTRATANTE - ASSEMBLÉIA LEGISLATIVA DA BAHIA

C.N.P.J. - 14.674.337/0001-99

**CONTRATADA - VTECH COMÉRCIO SERVIÇOS E EQUIPAMENTOS DE
INFORMÁTICA EIRELI - EPP**

C.N.P.J. - 22.122.370/0001-34

**ENDEREÇO - AVENIDA SANTOS DUMONT, 4487, KM3,5, LJ 157,
SHOPPING PASSEIO NORTE, ESTRADA DO COCO -
LAURO DE FREITAS/BA**

**OBJETO - AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA
ANTIVÍRUS PARA ESTAÇÕES DE TRABALHO,
MÁQUINAS SERVIDORES E MÁQUINAS SERVIDORES
VIRTUAIS.**

**VALOR - R\$ 64.900,00 (SESSENTA E QUATRO MIL E
NOVECENTOS REAIS)**

PROCESSO - Nº 2018000236

LICITAÇÃO - PREGÃO Nº 006/2018

**VIGÊNCIA - 12 (DOZE) MESES - A PARTIR DA DATA DE
ASSINATURA**

DOTAÇÃO ORÇAMENTÁRIA

ATIVIDADE - 7167

ELEMENTO - 3390.39

CONTRATO DE AQUISIÇÃO

Contrato nº **005/2018** que entre si celebram, de um lado, a **ASSEMBLÉIA LEGISLATIVA DO ESTADO DA BAHIA**, com sede na Av. Luis Viana Filho, - CAB, inscrita no CNPJ sob o nº 14.674.337/0001-99, neste ato representada pelo seu Presidente, Deputado Angelo Coronel, e doravante denominada simplesmente de **CONTRATANTE**, e do outro lado a empresa **VTECH COMÉRCIO SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA EIRELI - EPP**, estabelecida na Avenida Santos Dumont, 4487, KM3,5, LJ 157, Shopping Passeio Norte, Estrada Do Coco – Lauro De Freitas/BA, inscrita no CNPJ/MF sob o nº **22.122.370/0001-34**, neste ato representada por Natasha de Matos Oliveira Araújo, Sócia Administradora, e doravante designada de **CONTRATADA**.

CLÁUSULA PRIMEIRA DA REGÊNCIA LEGAL

O presente Contrato será regido pelo Pregão nº **006/2018**, processo nº **2018000236**, publicado em súmula no Diário Oficial do Estado da Bahia de 30/01/2018, do qual ele decorre e o integra independentemente de transcrição, pela Lei Federal nº 8.666/93, com as modificações subseqüentes, e pela da Lei Estadual nº 9.433/2005, pela proposta comercial apresentada pela Contratada e pelas seguintes cláusulas e condições:

CLÁUSULA SEGUNDA DO OBJETO

Constitui o objeto do presente Contrato é a aquisição de solução de segurança antivírus para estações de trabalho, máquinas servidores e máquinas servidores virtuais., conforme especificação constante no **PROJETO BÁSICO** e **ANEXO I** por menor preço global por lote, de acordo com as especificações nele indicadas.

A **CONTRATADA** ficará obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem no objeto, de até **25%(vinte e cinco por cento)** do valor inicial atualizado do contrato, na forma dos §1o e 2o do art. 143 da Lei Estadual nº 9.433/05.

CLÁUSULA TERCEIRA DOTAÇÃO ORÇAMENTÁRIA

As despesas para o pagamento deste contrato correrão por conta dos recursos da Dotação Orçamentária a seguir especificada: Atividade – **7167**, Elemento de Despesa – **3390.39**.

CLÁUSULA QUARTA DO PRAZO DE VIGÊNCIA CONTRATUAL

O presente Contrato terá a vigência de **12 (doze) meses** da data da assinatura podendo ser prorrogado por igual período até o prazo máximo de 60 (sessenta) meses, caso não haja manifestação contrária de nenhuma das partes.

CLÁUSULA QUINTA DO PREÇO, DAS CONDIÇÕES DE PAGAMENTO E DO REAJUSTE.

- a) Após a execução dos serviços e o exato cumprimento das obrigações assumidas, o pagamento será realizado pela Assembleia, através de depósito bancário em conta corrente, no valor total de **R\$ 64.900,00 (sessenta e quatro mil e novecentos reais)** até o **8º (oitavo) dia** contados da data do **ATESTO** ou **RECEBIDO** pelo setor competente, desde que não haja pendência a ser regularizada pelo contratado.
- b) Na hipótese de mora injustificada da **CONTRATANTE** no pagamento acordado, o preço contratado corresponderá ao respectivo valor corrigido financeiramente pelo IPG-DI – pro rata, excluídos do período de mora os dias em que tenha ocorrido atraso ou prorrogação na execução do Contrato. Multa moratória de **2% (dois por cento)**, mais encargos moratórios de **1% (um por cento)** ao mês pro rata die sobre o débito, ou outro crédito que venha a ser determinado pelo poder Concedente.
- c) A **CONTRATADA** aceita e se compromete, formal e solenemente, a não emitir duplicatas nem letras de câmbio contra a **CONTRATANTE**, nem tampouco colocar seus títulos, de qualquer espécie ou natureza, em cobrança bancária, obrigando-se a realizar todo e qualquer desempenho somente no seu órgão financeiro ou mediante empenho direto na praça de Salvador.
- d) As notas fiscais/faturas somente deverão ser apresentadas para pagamento após a entrega das licenças.
- e) O prazo de pagamento das notas fiscais/faturas será de 30 (trinta) dias após a apresentação das mesmas.
- f) Ainda que a nota fiscal/fatura seja apresentada antes do prazo definido para recebimento, o prazo para pagamento somente fluirá após o efetivo atesto do recebimento definitivo.
- g) As notas fiscais/faturas deverão estar acompanhadas da documentação probatória pertinente, relativa ao recolhimento dos impostos relacionados com a obrigação.
- h) Em havendo alguma pendência impeditiva do pagamento, a exemplo de erro na apresentação da nota fiscal/fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como obrigações financeiras

pendentes, decorrentes de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a **CONTRATADA** providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a **CONTRATANTE**.

i) As situações previstas na legislação específica sujeitar-se-ão à emissão de nota fiscal eletrônica.

j) A atualização monetária dos pagamentos devidos pela Administração, em caso de mora, será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do **INPC** do **IBGE** pró-rata tempore.

l) A Nota Fiscal/Fatura deverá conter, no mínimo, as seguintes informações:

l.1) Base de cálculo de impostos; Valor do imposto a ser pago.

m) Os preços aqui pactuados, conforme anexo I, sofrerão reajuste anual, para mais ou para menos, salvo disposição em contrário do Governo Federal, de acordo com a variação do **IGPM**, publicada pela Revista Conjuntura Econômica, da Fundação Getúlio Vargas.

n) O reajustamento de preços será efetuado na periodicidade prevista em lei federal, considerando-se a variação ocorrida desde a data da apresentação da proposta ou do orçamento a que esta se referir até a data do efetivo adimplemento da obrigação.

o) Os valores serão reajustados, em caso de renovação de contrato, pela variação do **INPC/IBGE** no período.

p) Quando, antes da data do reajustamento, tiver ocorrido revisão do contrato para manutenção do seu equilíbrio econômico financeiro, exceto nas hipóteses de força maior, caso fortuito, agravação imprevista, fato da administração ou fato do príncipe, será a revisão considerada à ocasião do reajuste, para evitar acumulação injustificada.

q) A atualização monetária dos pagamentos devidos pela Administração, em caso de mora, será calculada considerando a data do vencimento da fatura ou outro documento de cobrança e a do seu efetivo pagamento, de acordo com os critérios previstos no ato convocatório e que lhes preserve o valor. Para fins de atualização monetária dos débitos da Administração, será observado o prazo de até 08 (oito) dias úteis, contados da data de apresentação da Nota Fiscal/Fatura, ou outro documento de cobrança.

CLÁUSULA SEXTA DO PRAZO E LOCAL DE ENTREGA

A **CONTRATADA** deverá realizar a instalação da solução ofertada, em todas as estações de trabalho e servidores da **CONTRATANTE** de acordo com o número de licenças adquiridas, contemplando criação de novas regras, migração de regras e

políticas atualmente em utilização, em **até 30 (trinta) dias** após a publicação do extrato do Contrato no Diário Oficial do Estado da Bahia.

Deverá ser apresentado projeto técnico para aprovação pela **CONTRATANTE** antes do início das atividades, **no prazo máximo de 10 (dez) dias úteis** após a assinatura do contrato;

O objeto do presente Contrato será entregue à Diretoria de Tecnologia da Informação que procederá mensalmente a verificação e atesto dos serviços realizados.

CLÁUSULA SÉTIMA DA GARANTIA DO PRODUTO

- a) A solução deverá ter garantia total on-site de 01 (um) ano contado a partir da assinatura do contrato.
- b) Sem apresentar qualquer ônus à **CONTRATANTE**, a garantia deverá ser fornecida diretamente pelo fabricante da solução, e deverá abranger a manutenção corretiva com a cobertura de todo e qualquer defeito apresentado.
- c) A **CONTRATADA** deverá ser o único responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à **CONTRATANTE** ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante toda a vigência do contrato.
- d) A **CONTRATADA** é a única responsável pelos softwares fornecidos à **CONTRATANTE**, mesmo que tenham sido adquiridos de terceiros.
- e) Os serviços de garantia englobam todos os elementos de software da solução, incluindo a prestação de serviços de manutenção e assistência técnica, compreendendo a substituição de módulos, componentes, acessórios e aplicativos que apresentem defeito durante este período, sem qualquer ônus adicional para a **CONTRATANTE**, obrigando-se a **CONTRATADA** a manter todo o ambiente de antivírus corporativo permanentemente em perfeitas condições de funcionamento para a finalidade a que se destina, na forma estabelecida neste Termo;

CLÁUSULA OITAVA OBRIGAÇÕES DA CONTRATADA

1. É vedada a subcontratação parcial do objeto, a associação da contratada com outrem, a cessão ou transferência, total ou parcial do contrato, bem como a fusão, cisão ou incorporação da **CONTRATADA**, não se responsabilizando o contratante por nenhum compromisso assumido por aquela com terceiros;
2. Os serviços objeto deste contrato não podem sofrer solução de continuidade durante o prazo da sua vigência, devendo ser executados por empregados da **CONTRATADA**, sob a inteira responsabilidade funcional e operacional desta, mediante vínculo de

subordinação dos trabalhadores para com a empresa contratada, sobre os quais manterá estrito e exclusivo controle.

3. Fornecer todos os insumos previstos nos serviços agregados à modalidade de manutenção contratada, dentro dos prazos estabelecidos previamente com a **CONTRATANTE**, quando do surgimento da necessidade de prestação de quaisquer destes serviços;

4. Priorizar atendimento à **CONTRATANTE**, quando se tratar de chamado de urgência, que implique em paralisação das atividades da **CONTRATANTE**;

5. Fica expressamente proibida de utilizar qualquer informação fornecida pela **CONTRATANTE** sem prévia autorização por escrito, salvo nos casos em que esta informação derive apenas da experiência técnica decorrida da execução dos serviços;

6. A **CONTRATADA** deverá realizar a instalação da solução ofertada, em todas as estações de trabalho e servidores da **CONTRATANTE** de acordo com o número de licenças adquiridas, contemplando criação de novas regras, migração de regras e políticas atualmente em utilização, em até 30 (trinta) dias após assinatura do contrato;

7. Todo serviço de suporte e configuração deve ser realizado por profissional certificado pelo fabricante;

8. Deverá ser apresentado projeto técnico para aprovação pela **CONTRATANTE** antes do início das atividades, no prazo máximo de 10 (dez) dias úteis após a assinatura do contrato;

9. As atividades que possam causar impacto no ambiente de produção deverão ser realizadas fora do horário de expediente;

10. A **CONTRATADA** deverá realizar treinamento da solução ofertada para até 05 (cinco) pessoas, nas instalações da **CONTRATANTE**, sem qualquer ônus adicional para a última;

11. O treinamento será ministrado para a equipe de suporte técnico da **CONTRATADA** e deverá ser agendado em no máximo em 15 (quinze) dias após a instalação e aceite da solução;

12. O treinamento deverá possuir carga horária mínima de 20 (vinte) horas, e deverá abranger não apenas aspectos de instalação e configuração, mas também aspectos básicos e avançados da operação da solução, devendo ainda ser ministrado por instrutor com certificação técnica do seu fabricante.

13. As datas e os horários definidos para o treinamento deverão ser previamente aprovados pela **CONTRATANTE**.

14. Os chamados de assistência técnica, durante o período de garantia de 01 (um) ano, deverão ser abertos pela **CONTRATANTE**, junto à **CONTRATADA**, através de serviço telefônico 0800 ou de ligação com custo equivalente ao de chamada local;

15. Os serviços de abertura de chamados deverão estar disponíveis em regime 08x05;
16. Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentados. Esta documentação, bem como outras geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à **CONTRATANTE** através de relatórios (impressos e/ou em mídia digital) mediante solicitação;
17. A **CONTRATADA** deverá fazer análise dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe da **CONTRATANTE**;
18. A **CONTRATADA** deverá apresentar relatório contendo as ações adotadas para a solução de problemas encontrados, quando for o caso;
19. A manutenção corretiva, que se fará mediante chamado da **CONTRATANTE**, compreende quaisquer serviços que se fizerem necessários para manter a solução adquirida em perfeito estado de funcionamento, devendo a **CONTRATADA** atender, nas condições dos níveis de serviços estabelecidos neste Termo, a todo e qualquer chamado que venha a receber da **CONTRATANTE**;
20. Após a realização de manutenções corretivas, caberá ao técnico da **CONTRATADA** verificar a sua eficácia por meio de testes, em conjunto com o operador/usuário da **CONTRATANTE**, havendo a obrigatoriedade da assinatura de ambos no relatório ao final dos trabalhos;
21. Na manutenção corretiva a que se refere o item anterior, além dos testes a serem realizados, o técnico da **CONTRATADA** deverá acompanhar o funcionamento de todo o ambiente de antivírus, certificando-se de que o problema foi solucionado;
22. Os chamados para manutenção corretiva somente serão considerados atendidos após a conclusão dos reparos nos prazos estabelecidos neste Termo, sendo necessária a emissão de relatório após cada intervenção;
23. Deverão ser fornecidos à **CONTRATANTE** os dados necessários para identificação dos responsáveis pela manutenção dos equipamentos, inclusive endereço eletrônico (e-mail), número de telefone fixo, fax e celular;
24. Deverão ser prestadas, sempre que solicitado, orientações à equipe técnica da **CONTRATANTE**, ou seus usuários, pertinentes às funções da solução adquirida;
25. A **CONTRATADA** deverá fornecer atualizações automáticas das versões de software e manter a homogeneidade da ultima versão em todo o ambiente da solução fornecida;
26. Toda intervenção no ambiente da solução adquirida deverá ser comunicada e negociada previamente, para que sejam definidas a data e hora da sua realização;

27. A **CONTRATADA** deverá disponibilizar à **CONTRATANTE** o serviço de atendimento através de um gestor de contrato de suporte, que deverá ser o ponto focal de todas as necessidades de suporte da **CONTRATANTE** para casos de escalções ou problemas de atendimento do suporte técnico. Caso a **CONTRATADA** não possua laboratórios em território nacional, o referido gestor deverá ter fluência na língua portuguesa, a fim de facilitar a comunicação entre as partes;

28. A **CONTRATANTE** permitirá o acesso dos técnicos credenciados pela **CONTRATADA** às instalações onde se encontrarem os instalados os softwares e/ou equipamentos, para a prestação dos serviços de manutenção. No entanto, todo o pessoal da **CONTRATADA** ficará sujeito às normas internas de segurança da **CONTRATANTE**, notadamente àquelas atinentes à identificação, trânsito e permanência nas suas dependências;

29. Caso seja necessária a permanência do técnico da **CONTRATADA** nas instalações da **CONTRATANTE** além do tempo previsto para resolução do problema, tal fato não deverá representar qualquer ônus adicional à última;

30. Atendimento telefônico através de número 0800, ou serviço equivalente ao custo de chamada local, como serviço de uso ilimitado, no período de 08 (oito) horas por dia, 5 (cinco) dias por semana;

31. No Local (on-site) – Serviço de uso ilimitado, prestado em caso de emergência ou outra necessidade maior, e também compreendendo os seguintes tipos de atendimento local: suporte para upgrade de versões e releases do software; solução de problemas detectados (troubleshooting); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; e atualização simultânea nos ambientes dos órgãos e unidades da **CONTRATANTE**.

32. Para efeito dos atendimentos técnicos, a **CONTRATADA** deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

| NÍVEIS DE SEVERIDADE DOS CHAMADOS | |
|-----------------------------------|---|
| Nível | Descrição |
| 1 | Serviços totalmente indisponíveis. |
| 2 | Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos. |
| 3 | Serviços disponíveis com ocorrência de alarmes de avisos, consultas sobre problemas e dúvidas gerais. |

| Tabela de Prazos de Atendimento ao Software | | | | |
|---|---------------------|----------------------|---------|----------|
| Modalidade | Prazos | Níveis de Severidade | | |
| | | 1 | 2 | 3 |
| On-site | Início atendimento | 1 hora | 2 horas | 24 horas |
| | Término atendimento | 2 horas | 4 horas | 72 horas |
| Telefone, e-mail e web | Início atendimento | - | - | 24 horas |
| | Término atendimento | - | - | 72 horas |

Observações:

1) Para casos de severidade de nível 1, caso o atendimento não seja finalizado até as 20h00min, o técnico não poderá interrompê-lo, devendo continuá-lo até sua finalização, exceto quando explicitamente autorizado pela **CONTRATANTE**, que determinará o momento posterior para continuação do atendimento.

2) Todo o chamado somente será caracterizado como “encerrado” mediante concordância da **CONTRATANTE**.

3) Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, esta deverá ser programada e planejada com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da **CONTRATANTE**.

33. A **CONTRATADA** deverá disponibilizar à **CONTRATANTE** um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução adquirida, inclusive de firmware, sem ônus para a **CONTRATANTE**;

34. No caso de necessidade de ações preventivas ou corretivas, a **CONTRATANTE** agendará com antecedência as implementações das correções junto à **CONTRATADA**, fora do horário comercial, preferencialmente em feriados e finais de semana, sem ônus para a **CONTRATANTE**;

35. A **CONTRATADA** deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução adquirida, sem ônus para a **CONTRATANTE** durante 01 (um) ano.

36. **Prestar suporte e manutenção preventivos da seguinte forma:**

1. Duas avaliações on-site do ambiente da **CONTRATANTE** a cada ano de contrato (uma por semestre), mediante verificação de instalações e configurações de toda a solução, adequando-as às melhores práticas de segurança. Esta atividade deverá gerar relatórios para acompanhamento pela equipe da **CONTRATANTE**;

2. Seis visitas técnicas on-site a cada ano de contrato (uma a cada dois meses), com duração de até 8 horas cada conforme a conveniência da **CONTRATANTE**, realizadas por profissionais certificados pelo fabricante para apoiar nas implementações e nos controles gerados pelas ações proativas.
37. Todo suporte deve ser prestado por técnicos certificados pelo fabricante.
38. A **CONTRATADA** deverá apresentar obrigatoriamente, comprovação de que possui em seu quadro técnico no mínimo um profissional com a certificação técnica do fabricante nas linhas de produtos ofertadas.
39. A **CONTRATADA** deverá apresentar os certificados dos técnicos e comprovação de vínculo destes com a empresa.
40. A **CONTRATADA** deverá executar o objeto no prazo acordado e de forma direta, sendo-lhe vedada a subcontratação.
41. Todos os componentes de software a serem utilizados na prestação dos serviços deverão ser testados por meio de procedimentos designados pela **CONTRATANTE**, findo os quais será elaborado relatório técnico com a análise dos resultados.
42. O processo de realização dos testes de verificação preliminar deverá ser desenvolvido de acordo com os eventos e atividades descritos a seguir:
- 42.1. Testes de Instalação: consiste na verificação da instalação e da configuração das funcionalidades instaladas;
- 42.2. Testes de Ativação: consiste na operacionalização do software, após a conclusão dos testes de instalação, com a verificação de suas características, de suas funcionalidades e de sua compatibilidade.
43. A **CONTRATADA** fornecerá, por sua conta, instalações, configurações e licenças de todos os softwares que se fizerem necessários para a execução contratual da prestação de serviços decorrentes deste Termo de Referência.
44. Qualquer instalação de software em ambiente da **CONTRATADA** será precedida de justificativa, e somente será autorizado se for compatível com as exigências da **CONTRATANTE** e de seu provedor. Necessidades outras, além das descritas acima, serão arcadas pela própria **CONTRATADA**, as quais não serão passíveis de cobranças adicionais.
45. A **CONTRATADA** entregará à **CONTRATANTE** toda e qualquer documentação gerada em função da prestação de serviços decorrente deste Termo de Referência.
46. A **CONTRATADA** concorda que os direitos patrimoniais autorais relativos aos resultados produzidos durante a vigência do Contrato serão de propriedade exclusiva da **CONTRATANTE**, devidamente amparada pela Lei nº 9.610/1998, de Direitos Autorais, respeitados os direitos morais do autor. Entendem-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados,

esquemas, plantas, desenhos, diagramas, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica.

47. A **CONTRATADA** ficará proibida de veicular e comercializar todos e quaisquer produtos e informações geradas ou conhecidas relativas ao objeto da prestação dos serviços, salvo se houver a prévia autorização por escrito da **CONTRATANTE**.

CLÁUSULA NONA OBRIGAÇÕES DA CONTRATANTE

- a) A **CONTRATANTE** obriga-se a publicar o resumo do Contrato no Diário Oficial do Estado da Bahia, até o quinto dia do mês seguinte ao da sua assinatura contando que isto ocorra dentro de 10 (dias) a contar da referida assinatura.
- b) A **CONTRATANTE** se obriga a permitir livre acesso às informações, documentos e materiais necessários à execução dos serviços objeto deste contrato;
- c) Disponibilizar, para efeito da execução das atividades previstas neste contrato, toda a documentação da rede existente, incluindo plantas, relação de pontos com suas respectivas localizações, além dos pontos da rede devidamente identificados e sem duplicidade;
- d) Caso a **CONTRATANTE** não disponha da referida documentação, caberá a ela a contratação dos serviços relativos ao seu fornecimento, antes do início das atividades de manutenção, previstas neste contrato;
- e) A **CONTRATANTE** obriga-se a seguir os procedimentos de segurança indicados pela **CONTRATADA** para a melhor conservação dos materiais submetidos à manutenção aqui pactuada. Qualquer serviço decorrente de falhas nestes procedimentos não será considerado como do âmbito deste contrato, ficando, portanto, sujeito a restituição dos custos envolvidos, de acordo com a tabela de preços vigente na ocasião da realização dos mesmos.

CLÁUSULA DÉCIMA DAS PENALIDADES, DA INEXECUÇÃO E DA RESCISÃO.

A inexecução, total ou parcial, do Contrato ensejará a suspensão, a imposição da declaração de inidoneidade para licitar e contratar com o Estado da Bahia, multa, ou a sua rescisão, observadas, para tanto, as disposições da Sessão VIII, capítulo IX, da Lei Estadual n.º 9.433/2005.

O descumprimento, parcial ou total, de qualquer das cláusulas contidas no Contrato sujeitará o Contratado às sanções previstas na Lei Estadual n.º 9.433/2005, garantida a prévia e ampla defesa em processo administrativo.

A Administração se reserva ao direito de descontar do pagamento devido à **CONTRATADA** o valor de qualquer multa porventura imposta em virtude do descumprimento das condições estipuladas no Contrato.

As multas previstas nesta cláusula não têm caráter compensatório e o seu pagamento não eximirá o Contratado da responsabilidade de perdas e danos decorrentes das infrações cometidas.

A **CONTRATANTE** poderá rescindir administrativamente o Contrato nas hipóteses previstas na Lei Estadual n.º 9.433/2005.

CLÁUSULA DÉCIMA PRIMEIRA DO EXERCÍCIO DOS DIREITOS

Qualquer omissão ou tolerância das partes ao exigir o estrito cumprimento dos termos e condições deste Contrato, anexos e aditivos, ou o exercício de prerrogativa deles decorrentes, não constituirá renúncia ou novação nem afetará o direito das partes contratantes em exercê-lo a qualquer tempo.

CLÁUSULA DÉCIMA SEGUNDA COBRANÇA JUDICIAL

As importâncias devidas pela **CONTRATADA** serão cobradas através de processo de execução, constituindo este contrato, título executivo extrajudicial, ressalvada a cobrança direta, mediante retenção ou compensação de créditos, sempre que possível.

CLÁUSULA DÉCIMA TERCEIRA FORO CONTRATUAL

Fica eleito o Foro da Comarca de Salvador, Capital do Estado da Bahia, para dirimir todas as questões oriundas do presente contrato.

CLÁUSULA DÉCIMA QUARTA DAS DISPOSIÇÕES FINAIS

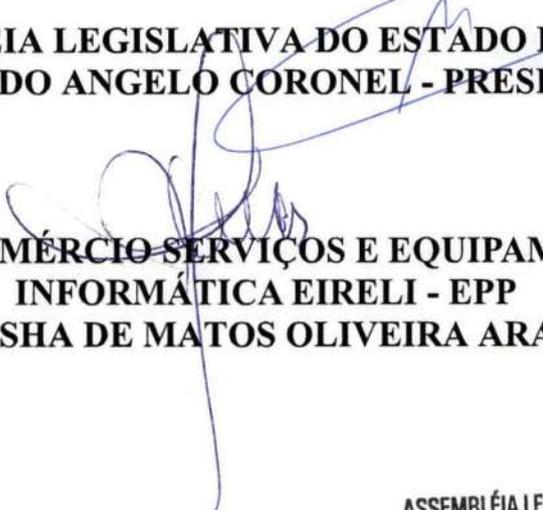
Será aplicado a este Contrato no que se refere a sua execução, bem como aos casos omissos, a Lei Estadual nº 9.433/2005.

A ausência ou omissão da fiscalização pela **CONTRATANTE**; não eximirá a **CONTRATADA** das responsabilidades previstas neste contrato.

E por estarem assim justas e contratadas assinam este instrumento em 03 (três) vias de igual forma e teor, que vão também subscritas por 02 (duas) testemunhas a fim de que se produzam seus efeitos de direito.

Salvador, 23 de Março de 2018.

ASSEMBLEIA LEGISLATIVA DO ESTADO DA BAHIA
DEPUTADO ANGELO CORONEL - PRESIDENTE


VTECH COMÉRCIO SERVIÇOS E EQUIPAMENTOS DE
INFORMÁTICA EIRELI - EPP
NATASHA DE MATOS OLIVEIRA ARAÚJO

ASSEMBLÉIA LEGISLATIVA DO ESTADO DA BAHIA
Registro às fs. 04 do Livro 28
Bahia 27 de Março de 2018

FUNCIONÁRIO

TESTEMUNHAS:

1 -

2 -

ANEXO I

ITEM 01 – Solução Antivírus para estações de trabalho e máquinas servidores deverá atender as seguintes especificações:

2. Especificações técnicas

- 1.1.1 - Licenciamento de uso do software para 1.200 (mil e duzentas) estações de trabalho e 10 servidores físicos, sendo 5 servidores Windows e 5 servidores Linux;
- 1.1.2 - Upgrade de versões e atualizações do software de antivírus por 01 (um) ano, sem custos adicionais;
- 1.1.3 - Atualizações das definições de malware por 01 (um) ano, sem custos adicionais;
- 1.1.4 - Suporte em português do Brasil, oferecido pelo próprio fabricante, representante ou parceiro certificado do software de antivírus, por telefone 08x05 e, quando necessário, presencialmente nas instalações da CONTRATANTE, conforme as especificações de níveis de serviço deste Termo;
- 1.1.5 - Ser compatível para instalação em estações de trabalho e servidores com os seguintes sistemas operacionais: Microsoft Windows 7 (32 e 64 bits); Microsoft Windows 7 SP1 (32 e 64 bits); Microsoft Windows 8 (32 e 64 bits); Microsoft Windows 10 ou mais recente; Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2 e 2016; Microsoft Small Business Server 2008 e 2011; CentOS 6.7, 6.8 e 7.3; Debian 7.10, 7.11, 8.5 e 8.6; Oracle Linux 6.7, 6.8 RHCK, 7.2 e 7.3 UEK; Red Hat Enterprise Linux 6.7, 6.8, 7.2 e 7.3; SUSE Linux Enterprise Server 11 SP3 e SP4, 12 e 12 SP1; Ubuntu 14.04.(4-5), 16.04, 16.04.1 e 16.04.2; Amazon Linux 2017.03.
- 1.1.6 - Servidor de gerenciamento instalável em Windows Server 2008 SP1 (64 bits) versões: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server; Windows Server 2008 R2 e 2008 R2 SP1 versões: Standard, Enterprise e Web Server; Windows Server 2012 e 2012 R2 versões: Essentials, Standard e Datacenter; Windows Server 2016 versões Essentials, Standard e Datacenter; Linux 64 bits nas seguintes distribuições: Red Hat Enterprise Linux 5, 6 e 7; CentOS 6 e 7; OpenSUSE 13.2; SUSE Linux Enterprise Server 10 e 11; SUSE Linux Enterprise Desktop 11; Debian GNU Linux 7, 8 e 9; Ubuntu 12.04, 14.04 e 16.04.
- 1.1.7- Console de Gerenciamento instalável em todas as plataformas do servidor de gerenciamento, além das seguintes plataformas: Windows 7 e Windows 7 SP1



(64 bits) versões: Professional, Enterprise e Ultimate; Windows 8 (64 bits); Windows 8.1 (64 bits); Windows 10.(64 bits);

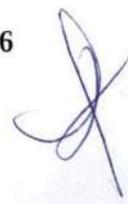
- 1.1.8 - Todas as funcionalidades devem ser ativadas por agente de modo a facilitar a instalação, a configuração e o gerenciamento;
- 1.1.9 - Ser composto de software dedicado à proteção contra diversos tipos de malware, tais como vírus, spyware, adware, worm, rootkit e vulnerabilidades zero-hour para estações de trabalho e servidores;
- 1.1.10 - Detectar e remover malwares localizados em drives locais, diretórios e subdiretórios, mídias removíveis, programas executáveis, setores de BOOT e vírus de macro;
- 1.1.11 - Permitir a instalação remota do software via console, por script de login ou Política de Grupo (GPO), e impedir a interrupção do processo de instalação ou a sua desinstalação pelo usuário;
- 1.1.12 - Toda a solução de segurança para estações de trabalho e servidores físicos do Item 01 deste lote deverá ser fornecida por um único fabricante, de modo que tanto o suporte à solução quanto as suas funcionalidades sejam inteiramente integradas e gerenciadas através de um único console de gerenciamento;
- 1.1.13 - O software antivírus para estações e servidores deverá ser baseado em três níveis: console de gerenciamento, servidores de gerenciamento e agente de comunicação entre cliente antivírus e servidor antivírus;
- 1.1.14 - A conexão entre o cliente e o servidor antivírus deverá suportar configurações sobre os protocolos TCP/IP;
- 1.1.15 - A proteção anti-spyware deverá ser nativa da própria solução, isto é, não poderá depender de plugin ou módulo adicional;

1.2 - Solução para servidores Windows

- 1.2.1 - Possuir a capacidade de atualizar remotamente e em tempo real, as listas de definições de malware, sem a necessidade de utilização de login-scripts, agendamentos ou intervenções do usuário;
- 1.2.2 - Possuir capacidade de programação de atualizações das listas de definições de malware, a partir de local predefinido da rede ou site da Internet;
- 1.2.3 - Possuir capacidade de atualização das listas de definições de malware por meio de um servidor proxy, fornecido pelo fabricante da solução, para redução do consumo de banda em sites remotos;
- 1.2.4 - Possuir atualização incremental das assinaturas nas estações de trabalho;



- 1.2.5 - O sistema de antivírus ofertado deve permitir a programação de, no mínimo, duas ações automáticas (primária e secundária), para o caso de detecção de malware, com as seguintes opções:
- 1.2.5.1 - Somente alertar;
 - 1.2.5.2 - Limpar automaticamente;
 - 1.2.5.3 - Apagar automaticamente;
 - 1.2.5.4 - Colocar em quarentena (isolar);
- 1.2.6 - Possibilitar a tomada de ações independentes para casos de detecção de malware;
- 1.2.7 - Relatar para o console de gerenciamento todos os tipos de programas potencialmente perigosos (ex: spyware) para que sua utilização possa ser definida (liberada ou bloqueada) pelo administrador;
- 1.2.8 - Possuir controle de aplicativos que acessam a rede, reportando todos eles para o console de gerenciamento, de forma que o administrador possa controlar sua utilização pelos usuários (liberar ou bloquear a abertura e o recebimento de conexões);
- 1.2.9 - Possibilitar acionamento de função de verificação do sistema de forma manual, pré-agendada ou em tempo real contra vírus, worms, cavalos de troia e demais tipos de códigos maliciosos;
- 1.2.10 - Possuir proteção em tempo real contra vírus, worms, cavalos de troia, spywares, adwares, e demais tipos de códigos maliciosos, integrada em uma única solução independente de plugin ou módulo adicional;
- 1.2.11 - Possuir proteção contra rootkits;
- 1.2.12 - Detectar e remover cookies potencialmente indesejáveis no sistema (ex: cookies de rastreamento);
- 1.2.13 - Permitir a verificação em tempo real e a verificação manual de todos os tipos de arquivos, bem como a definição dos tipos de arquivos a serem verificados contra malware;
- 1.2.14 - Permitir a criação de listas de exclusões de objetos da varredura (diretórios, arquivos e extensões de arquivos);
- 1.2.15 - Realizar verificação e proteção do sistema de registro (registry) contra modificações não autorizadas;
- 1.2.16 - Reconhecer e impedir, através de análise heurística, a ação de software malicioso ao tentar executar funções que possam causar dano ao sistema, tais como alterar o registro do sistema operacional e associações críticas a arquivos,



com capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema;

- 1.2.17 - Possuir rastreamento manual, disparado pelo usuário, com interface gráfica e opções de seleção de arquivos, diretórios ou discos a serem analisados, ou de varredura completa da estação, inclusive com verificação de rootkits;
- 1.2.18 - Detectar novos tipos de ameaças, ainda desconhecidas, como spyware, adware, jokes, dialers, remote access, trackware e ferramentas de hack através de análise heurística de comportamento;
- 1.2.19 - Permitir o envio de amostras de arquivos suspeitos para análise do fabricante;
- 1.2.20 - Deve possuir a capacidade de detectar a origem de ameaças na rede, fornecendo informações como endereço IP e nome DNS / NetBios;
- 1.2.21 - Realizar o rastreamento em tempo real, para arquivos criados, copiados, renomeados, movidos ou modificados;
- 1.2.22 - Realizar a verificação de malware em arquivos compactados em pelo menos 05 (cinco) níveis de profundidade;
- 1.2.23 - Possuir, no mínimo, 02 (dois) mecanismos (engines) anti-malware trabalhando simultaneamente e gerenciados através do mesmo console de gerenciamento;
- 1.2.24 - Gerar registro (log) dos eventos de detecção de malware em arquivo em local definido pelo usuário;
- 1.2.25 - Possuir geração e exibição de alertas em caso de detecção de malware, através de mensagem na tela, no console de administração e no sistema de registro de eventos da estação, via SNMP e e-mail SMTP;

1.3 - Solução para estações de trabalho Windows

- 1.3.1 - Possuir a capacidade de atualizar remotamente e em tempo real, as listas de definições de malware, sem a necessidade de utilização de login-scripts, agendamentos ou intervenções do usuário;
- 1.3.2 - Possuir capacidade de programação de atualizações das listas de definições de malware, a partir de local predefinido da rede ou site da Internet;
- 1.3.3 - Possuir capacidade de atualização das listas de definições de malware por meio de um servidor proxy, fornecido pelo fabricante da solução, para redução do consumo de banda em sites remotos;
- 1.3.4 - Possuir atualização incremental das assinaturas nas estações de trabalho;



- 1.3.5 - Possuir solução de reputação WEB, integrada e gerenciada através da solução de antivírus, cancelando conexões prejudiciais de forma automática, com base na resposta à consulta da base do fabricante;
- 1.3.6 - Possuir recurso de proteção contra exploits inseridos em páginas e scripts WEB.
- 1.3.7 - O sistema de antivírus ofertado deve possuir a possibilidade de programar no mínimo duas ações automáticas (primária e secundária), para o caso de detecção de malware, com as seguintes opções:
 - 1.3.7.1 - Somente alertar;
 - 1.3.7.2 - Limpar automaticamente;
 - 1.3.7.3 - Apagar automaticamente;
 - 1.3.7.4 - Colocar em quarentena (isolar).
- 1.3.8 - Possibilitar a tomada de ações independentes para casos de detecção de malware;
- 1.3.9 - Relatar para o console de gerenciamento todos os tipos de programas potencialmente perigosos (ex: spyware) para que sua utilização possa ser definida (liberada ou bloqueada) pelo administrador;
- 1.3.10 - Possuir controle de aplicativos que acessam a rede, reportando todos eles para o console de gerenciamento, de forma que o administrador possa controlar sua utilização pelos usuários (liberar ou bloquear a abertura e o recebimento de conexões);
- 1.3.11 - Possibilitar acionamento de função de verificação do sistema de forma manual, pré-agendada ou em tempo real contra vírus, worms, cavalos de troia e demais tipos de códigos maliciosos;
- 1.3.12 - Possuir proteção em tempo real contra vírus, worms, cavalos de troia, spywares, adwares, e demais tipos de códigos maliciosos, integrada em uma única solução independente de plugin ou módulo adicional;
- 1.3.13 - Possuir proteção contra rootkits;
- 1.3.14 - Detectar e remover cookies potencialmente indesejáveis no sistema (ex: cookies de rastreamento);
- 1.3.15 - Permitir a verificação em tempo real e a verificação manual de todos os tipos de arquivos, bem como a definição dos tipos de arquivos a serem verificados contra malware;
- 1.3.16 - Permitir a criação de listas de exclusões de objetos da varredura (diretórios, arquivos e extensões de arquivos);



- 1.3.17 - Realizar verificação e proteção do sistema de registro (registry) contra modificações não autorizadas;
- 1.3.18 - Reconhecer e impedir, através de análise heurística, a ação de software malicioso ao tentar executar funções que possam causar dano ao sistema, tais como alterar o registro do sistema operacional e associações críticas a arquivos, com capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema;
- 1.3.19 - Possuir rastreamento manual, disparado pelo usuário, com interface gráfica e opções de seleção de arquivos, diretórios ou discos a serem analisados, ou de varredura completa da estação, inclusive com verificação de rootkits;
- 1.3.20 - Detectar novos tipos de ameaças, ainda desconhecidas, como spyware, adware, jokes, dialers, remote access, trackware e ferramentas de hack através de análise heurística de comportamento;
- 1.3.21 - Deve possuir módulo para varredura do tráfego HTTP durante a navegação via browser analisando o tráfego em busca de códigos maliciosos
- 1.3.22 - A solução deve possuir a capacidade de bloqueio de URL's, incluindo bloqueio de URL's que utilizem o protocolo HTTPS para navegação
- 1.3.23 - Permitir o envio de amostras de arquivos suspeitos para análise do fabricante;
- 1.3.24 - Possuir IDS (intrusion detection system), integrado com firewall pessoal e gerenciado pelo mesmo console do mesmo fabricante da solução de antivírus, com atualização automática;
- 1.3.25 - Permitir a definição de novos serviços baseados nos protocolos e portas utilizados;
- 1.3.26 - Permitir a definição de regras para permissão/negação de acesso baseadas nos serviços, origem e destino das conexões;
- 1.3.27 - Possibilitar a definição de múltiplas políticas, utilizando as regras definidas;
- 1.3.28 - Possibilitar a aplicação de diferentes políticas para grupos de estações ou estações específicas;
- 1.3.29 - Viabilizar o controle de aplicativos nas estações de trabalho, listando os softwares confiáveis que trafegam pela rede, desta forma bloqueando o tráfego desnecessário gerado por softwares não autorizados;
- 1.3.30 - Deve possuir a capacidade de detectar a origem de ameaças na rede, fornecendo informações como endereço IP e nome DNS / NetBios;
- 1.3.31 - Realizar o rastreamento em tempo real, para arquivos criados, copiados, renomeados, movidos ou modificados;



- 1.3.32 - Possibilitar acionamento de função de verificação de ocorrência de malware de forma manual, pré-agendada ou em tempo real;
- 1.3.33 - Possuir, no mínimo, 02 (dois) mecanismos (engines) anti-malware trabalhando simultaneamente e gerenciados através do mesmo console de gerenciamento;
- 1.3.34 - Gerar registro (log) dos eventos de detecção de malware em arquivo em local definido pelo usuário;
- 1.3.35 - Possuir geração e exibição de alertas em caso de detecção de malware, através de mensagem na tela, no console de administração e no sistema de registro de eventos da estação, via SNMP e e-mail SMTP;
- 1.3.36 - Possuir interface do usuário no idioma Português (Brasil) ou Inglês;
- 1.3.37 - Ser capaz de detectar malwares durante a navegação web de forma independente do navegador web, interceptando e verificando o tráfego do protocolo HTTP;
- 1.3.38 - Impedir a execução de componentes ActiveX;
- 1.3.39 - Agregar proteção integrada aos browsers Internet Explorer e Mozilla Firefox contra sites maliciosos, com sistema de reputação. A proteção deve conectar-se à nuvem onde deverá haver lista atualizada de websites maliciosos;
- 1.3.40 - Classificar resultados de pesquisas em sites de busca como Google, Yahoo, etc., de acordo com a reputação do site, indicando para o usuário a classificação de cada resultado através de informações na tela;
- 1.3.41 - Bloquear sites (páginas) que contenham vulnerabilidades detectadas pelo módulo de proteção a navegação;
- 1.3.42 - Mostrar a classificação de links em serviços de e-mail via web (webmails);
- 1.3.43 - Permitir ao administrador liberar o acesso a páginas bloqueadas automaticamente pela solução, caso entenda que as mesmas não oferecem risco aos usuários;
- 1.3.44 - Permitir a atualização de um determinado segmento de rede através de estações de trabalho eleitas para serem os repositórios deste segmento, sem a necessidade de instalação de um módulo adicional nas estações ou servidores para realizar esta tarefa;
- 1.3.45 - Permitir a definição de um adaptador de rede confiável, onde o tráfego de e/ou para este adaptador não será bloqueado pelo firewall;
- 1.3.46 - Possuir módulo de controle de aplicativos, bloqueando-os mesmo se os seus nomes forem alterados pelo usuário, e viabilizando seu gerenciamento através



do mesmo console de gerenciamento dos módulos antivírus, anti-spyware e firewall;

- 1.3.47 - Possuir controle de todos os aplicativos que acessam recursos de rede em cada uma das estações de trabalho, informando a sua existência ao console de administração e permitindo ao administrador definir quais destes aplicativos podem ou não ser executados. Permitir ao administrador definir mensagens a serem apresentadas para os usuários nos casos de bloqueio de aplicações;
- 1.3.48 - Permitir habilitar/desabilitar dispositivos de hardware externo (USB) por tipo específico, classe e subclasse de dispositivo nas estações de trabalho.
- 1.3.49 - Permitir bloquear dispositivos no mínimo pelo Hardware ID, ID do dispositivo, ID compatível e Classe GUID
- 1.3.50 - Permitir bloquear dispositivos como, no mínimo, Modems 3G, Dispositivos de armazenamento em massa, câmeras de vídeo embutidas e móveis, mouse com e sem fio, teclados, cd-rom, leitores de cartão, leitores de discos flexíveis (disquetes), discos rígidos (Hds)
- 1.3.51 - O bloqueio de dispositivos deve permitir bloquear um único dispositivo e liberar todos os demais, bem como liberar um único dispositivo e bloquear os demais. Ex.: Bloquear qualquer Pendrive exceto um em um único computador
- 1.3.52 - As regras de bloqueio de dispositivos devem permitir ser aplicadas por grupo, host e todo o domínio

1.4 - Solução para servidores e estações de trabalho GNU/Linux

- 1.4.1 - O sistema de antivírus, anti-spyware, anti-rootkit e firewall integrado para servidores de arquivos Linux deve ser fornecido em um único pacote de instalação para ambientes de servidores e de estações de trabalho;
- 1.4.2 - Deverá possibilitar varredura em tempo real para arquivos durante a sua leitura e escrita, com, no mínimo, as seguintes opções:
 - 1.4.2.1 - Renomear o arquivo infectado;
 - 1.4.2.2 - Desinfetar o arquivo infectado;
 - 1.4.2.3 - Apagar o arquivo infectado;
 - 1.4.2.4 - Colocar o arquivo infectado em quarentena.
- 1.4.3 - Rastreamento manual através da interface gráfica e de linha de comando (CLI) local, personalizável;
- 1.4.4 - Rastreamento em tempo real dos processos em memória;
- 1.4.5 - Possuir capacidade de programação de atualizações das listas de definições de malware, a partir de local predefinido da rede ou site da Internet;



- 1.4.6 - Possuir atualização incremental das assinaturas nas estações de trabalho;
- 1.4.7 - Salvar automaticamente as listas de definições de malware no repositório central da rede;
- 1.4.8 - Programação de rastreamento automático do sistema:
 - 1.4.8.1 - Ação: Somente alertar, limpar automaticamente, apagar automaticamente ou renomear automaticamente;
 - 1.4.8.2 - Frequência: Horária, diária, semanal, mensal;
 - 1.4.8.3 - Exclusões: Pastas ou arquivos que não devem ser rastreados.
- 1.4.9 - Gerar registro (log) dos eventos de detecção de malware em arquivo;
- 1.4.10 - Gerar notificações de eventos de malware através de alerta na rede;
- 1.4.11 - Capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema através de análise heurística;
- 1.4.12 - Possuir ferramenta de segurança que assine e verifique a integridade dos módulos do kernel, possibilitando alteração mediante autorização do administrador;
- 1.4.13 - Rastreamento em tempo real de discos contra spyware, com pelo menos as seguintes opções:
 - 1.4.13.1 - Apagar o spyware;
 - 1.4.13.2 - Mover o spyware para a quarentena.
- 1.4.14 - Detecção de cookies potencialmente indesejáveis no sistema (ex: cookies de rastreamento);
- 1.4.15 - Rastreamento em tempo real dos processos em memória contra spywares;
- 1.4.16 - Programação de rastreamento manual do sistema:
 - 1.4.16.1 - Escopo: Todos os drives locais, drives específicos, ou pastas específicas;
 - 1.4.16.2 - Ação: Somente alertar, limpar automaticamente, apagar automaticamente;
 - 1.4.16.3 - Exclusões: Pastas ou arquivos que não devem ser rastreados.
- 1.4.17 - Atualização incremental da lista de ameaças;
- 1.4.18 - Possuir gerenciamento centralizado, permitindo a configuração de recursos antivírus e anti-spyware através da mesma interface de gerenciamento utilizada para as soluções Windows;



1.4.19 - Possuir IDS (intrusion detection system), integrado com firewall pessoal e gerenciado pelo mesmo console da solução de antivírus;

1.4.20 - Permitir a utilização de interface de linha de comando (CLI) para as ações de proteção;

1.4.21 - Possuir capacidade de criar baseline de assinatura arquivos de sistema (kernel, etc.) impedindo a modificação e a atualização indevidas do sistema operacional. As modificações e atualizações do sistema devem ser permitidas pelo administrador através do console de gerenciamento.

1.5 - Módulo para gerenciamento da solução antivírus – gerência centralizada de todos os módulos da suíte:

1.5.1 - Deve permitir a instalação do servidor de gerenciamento em todas as plataformas indicadas na seção inicial do Item 01 do Lote 01;

1.5.2 - Deve permitir a instalação do console de gerenciamento em todas as plataformas indicadas na seção inicial do Item 01 do Lote 01;

1.5.3 - Deve administrar toda a solução ofertada, inclusive estações de trabalho e servidores Linux;

1.5.4 - Deve possuir interface única para configuração de políticas para antivírus, anti-spyware, firewall e IDS;

1.5.5 - Utilizar chave de criptografia para garantir segurança de comunicação entre o servidor de gerenciamento, o console de gerenciamento e as estações de trabalho. Toda a troca de informação entre qualquer dos componentes da solução deve ser assinada digitalmente para garantir a origem da informação;

1.5.6 - Executar a comunicação com estações de trabalho, servidores e servidor de gerenciamento através do protocolo HTTP, em portas definidas pelo administrador;

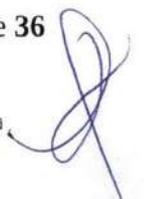
1.5.7 - Permitir a criação de grupos de estações, definidos pelo administrador;

1.5.8 - Permitir o gerenciamento dos produtos antivírus como uma árvore de diretórios, personalizada pelo administrador;

1.5.9 - Exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da estação, versão do antivírus, data das definições de malware, data da última verificação e status (infectada por malware, desatualizada etc.);

1.5.10 - Detecção de domínios e grupos de trabalho a partir da estrutura de diretórios pré-existentes do active directory;

1.5.11 - Agrupar estações de trabalho por domínio ou grupo, ou permitir definir qual domínio ou grupo a estação irá pertencer



- 1.5.12 - Configuração diferenciada para cada estação, grupo de estações, domínio ou grupos de domínios
- 1.5.13 - Possuir gerenciamento e configuração remota para a funcionalidade de controle de aplicativos e firewall
- 1.5.14 - Possuir gerenciamento e configuração remota para a funcionalidade de Zero Hour e/ou Zero Day
- 1.5.15 - Possuir gerenciamento e configuração remota para a funcionalidade de Quarentena de rede
- 1.5.16 - Deve ser capaz de bloquear as configurações nas estações de trabalho sem a necessidade de senha, evitando que os usuários alterem as configurações do produto
- 1.5.17 - Permitir a visualização das características das estações como: nome de rede, IP e sistema operacional;
- 1.5.18 - Bloquear o acesso às configurações e remoção do software antivírus pelo usuário final, através de políticas definidas pelo administrador;
- 1.5.19 - Aplicar mudanças nas configurações do antivírus, para todos os computadores, por grupo de computadores ou individualmente por computador;
- 1.5.20 - Forçar a configuração determinada no servidor para as estações clientes;
- 1.5.21 - Permitir a instalação e atualização do software sem a intervenção do usuário;
- 1.5.22 - Possibilitar a identificação de estações de trabalho que ainda não possuem o software de proteção ativo;
- 1.5.23 - Possibilitar a programação e execução de rastreamento remoto contra malware, com a opção de selecionar uma estação ou um grupo de estações para rastreamento;
- 1.5.24 - Realizar o gerenciamento centralizado da área de quarentena;
- 1.5.25 - Emitir relatórios sobre o status de toda a solução instalada;
- 1.5.26 - Gerar relatórios gráficos através de interface WEB;
- 1.5.27 - Permitir a exportação dos relatórios para pelo menos um dos formatos a seguir: HTML, XML e CSV;
- 1.5.28 - O sistema de antivírus ofertado deve permitir a geração de relatórios que contenham as seguintes informações:
 - 1.5.28.1 - Lista de estações com as definições de malwares desatualizadas;
 - 1.5.28.2 - Versão do software de antivírus instalado em cada estação;
 - 1.5.28.3 - Lista de malwares com maior número de detecções;

- 1.5.28.4 - Lista de estações que mais sofreram infecções, em determinado período de tempo;
- 1.5.28.5 - Estado da comunicação entre as estações clientes e o servidor de gerência;
- 1.5.28.6 - Distribuição das listas de definições e mecanismo de varredura nas estações clientes;
- 1.5.28.7 - Sumário dos produtos antivírus instalados;
- 1.5.28.8 - Versão do software de gerenciamento instalado;
- 1.5.28.9 - Ações tomadas pelo software antivírus;
- 1.5.28.10 - Histórico das infecções;
- 1.5.28.11 - Número de arquivos infectados detectados;
- 1.5.28.12 - Contagem de infecções por tipo de malware e período;
- 1.5.28.13 - Ranking das estações que mais sofreram ataque.
- 1.5.29 - Permitir o armazenamento das informações coletadas nas estações clientes em um banco de dados centralizado, sem a necessidade de aquisição de solução de banco de dados de terceiros, devendo este ser fornecido de forma integrada à solução antivírus, ofertada sem qualquer custo adicional;
- 1.5.30 - Permitir o acesso ao servidor de gerenciamento a partir de console instalado em outra estação;
- 1.5.31 - Permitir a instalação do antivírus nas estações clientes a partir de um único servidor, sem a necessidade de instalação prévia de um agente ou módulo;
- 1.5.32 - Permitir a alteração das configurações e políticas do antivírus nas estações clientes, de maneira remota;
- 1.5.33 - Permitir a execução de tarefas remotas de atualização, verificação de malware e upgrades, através do console de gerenciamento;
- 1.5.34 - Possibilitar a criação de grupos de estações baseadas em regras definidas pelo administrador;
- 1.5.35 - Forçar que as estações clientes recebam a configuração determinada através do servidor;
- 1.5.36 - Forçar a instalação do software antivírus nas estações clientes;
- 1.5.37 - Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou dial-up;
- 1.5.38 - Possuir a capacidade de gerar registros/logs para auditoria;
- 1.5.39 - Atualizar e implementar políticas de segurança proativas para toda a solução;



- 1.5.40 - Permitir a utilização de repositórios remotos para atualização, sem limite de instalação;
- 1.5.41 - Possibilitar o cadastro de vários administradores com permissão para acesso e configuração simultâneos;
- 1.5.42 - Permitir a importação da estrutura do Active Directory da Microsoft, de forma automática;
- 1.5.43 - Realizar a importação automática de novas estações com a instalação do produto baseado em regras, colocando-as no segmento da árvore de políticas definida pelo administrador;
- 1.5.44 - Remover automaticamente da árvore de políticas as estações que não estiverem mais presentes na rede;
- 1.5.45 - Todas as configurações dos softwares de antivírus deverão ser efetuadas no software de gerenciamento, e a sua aplicação nas estações deverá ser feita de forma automática, sem a necessidade de intervenção do usuário.

QUANTIDADE: 1.210 (UM MIL DUZENTOS E DEZ) LICENÇAS

VALOR UNITÁRIO R\$ 40,40 (QUARENTA REAIS E QUARENTA CENTAVOS)

VALOR TOTAL R\$ 48.884,00 (QUARENTA E OITO MIL, OITOCENTOS E OITENTA E QUATRO REAIS)

ITEM 02 - Solução Antivírus para Servidores Virtualizados

2 - O software para máquinas servidores virtuais deverá atender as seguintes especificações:

2.1 - Licenciamento de uso do software para 50 (cinquenta) servidores virtuais;

2.2 - A solução deve possuir tanto antivírus sem agentes (Agentless) como baseado em agentes para ambientes virtuais;

2.3 - A solução deve possuir gerenciamento, monitoramento e atualização de software e vacinas centralizados;

2.4 - A solução deve possuir capacidade de atualizar definições de vírus e padrões de ataques;

2.5 - Requerimentos para o antivírus sem agente:

2.5.1 - Software de antivírus sem agente para ambientes virtualizados deve funcionar com as seguintes versões do VMWARE:

2.5.1.1 - VMWARE ESXi Hypervisor 6.0;



- 2.5.1.2 - VMWARE ESXi Hypervisor 5.5 update 2;
 - 2.5.1.3 - VMWARE ESXi Hypervisor 5.1 update 3;
 - 2.5.1.4 - VMWARE vCenter 6.0.0a Server;
 - 2.5.1.5 - VMWARE vCenter Server 5.5 update 2e;
 - 2.5.1.6 - VMWARE vCenter Server 5.1 update 3a;
 - 2.5.1.7 - VMWARE vSphere Standard;
 - 2.5.1.8 - VSphere 6;
 - 2.5.1.9 - VMWARE vShield Endpoint do VMware vCloud Networking and Security 5.5.4.1 Suite;
 - 2.5.1.10 - VMware vShield Manager do VMware vCloud Networking and Security 5.5.4.1 Suite;
 - 2.5.1.11 - VMware NSX 6.x.
- 2.5.2 - Software de antivírus sem agente para ambientes virtuais deve proteger os seguintes sistemas operacionais para desktops:
- 2.5.2.1 - Windows 7 (x86 e x64);
 - 2.5.2.2 - Windows 8 (x86 e x64);
 - 2.5.2.3 - Windows 8.1 (x86 e x64) Quando utilizado com VMware vSphere 5.5 update 2 ou posterior;
- 2.5.3 - Software de antivírus sem agente para ambientes virtuais deve proteger os seguintes sistemas operacionais para servidores:
- 2.5.3.1 - Windows Server 2008 R2 (x64);
 - 2.5.3.2 - Windows Server 2012;
 - 2.5.3.3 - Windows Server 2012 sem ReFS (Resilient File system) suporte (x64);
 - 2.5.3.4 - Windows Server 2012 R2 (x64) Quando utilizado com o VMware vSphere 5.5 update 2 ou posterior;
 - 2.5.3.5 - Windows Server 2008 (x86 e x64);
 - 2.5.3.6 - Windows Server 2016
- 2.6 - O antivírus sem agente para ambientes virtuais deve prover as seguintes funcionalidades:**
- 2.6.1 - Proteção contra malware em tempo real e durante a verificação agendada sem a necessidade de qualquer agente instalado no computador convidado;

- 2.6.2 - Integração com a tecnologia VMware vShield Manager para proteger o sistema de arquivos do computador;
- 2.6.3 – Integração com a tecnologia VMware Network Extensibility SDK para prover proteção no nível de rede, implementado para monitorar e bloquear atividade maliciosa na rede bem como endereços de URL com a habilidade de notificar o usuário sobre os bloqueios efetuados;
- 2.6.4 - Proteção baseada em nuvem contra novas ameaças, permitindo a aplicação se comunicar com a fabricante do software para poder dar um veredito a um arquivo tanto na proteção em tempo real como na verificação agendada;
- 2.6.5 - Atualizações centralizadas no sistema com a proteção especializada para virtualização sem a necessidade de distribuir atualizações para cada máquina convidada;
- 2.6.6 - Possibilidade de verificação sob demanda ou manual nas máquinas virtuais selecionadas;
- 2.6.7 - Verificação de: arquivos selecionados, pastas ou todo o sistema na verificação agendada de todas as máquinas virtuais;
- 2.6.8 - Capacidade de implementar a solução de segurança sem a necessidade de reiniciar o Hypervisor ou entrar no modo de manutenção;
- 2.6.9 - Tecnologia que previne a verificação do mesmo arquivo mais de uma vez;
- 2.6.10 - Previne múltipla verificação em arquivos iguais mesmo que estejam em máquinas virtuais diferentes;
- 2.6.11 - Bloqueia, isola e remove vírus notificando o usuário e o administrador;
- 2.6.12 - Possui uma única console de gerenciamento para todos os componentes de proteção da solução do Lote II do Item 01;
- 2.6.13 - Uma única console de gerenciamento para o ambiente virtual;
- 2.6.14 - Capacidade de ver a estrutura de administração tanto física como lógica assim como é apresentado no VMware vCenter;
- 2.6.15 - Informações detalhadas sobre os eventos e tarefas de implementação nas máquinas virtuais;
- 2.6.16 - Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
- 2.6.17 - Cria exceções pelo nome do arquivo, pelo endereço dos arquivos e pela máscara dos arquivos;
- 2.6.18 - Permite exportar e importar listas de exceções;
- 2.6.19 - Cria lista de exceções frequentes de acordo com as recomendações da Microsoft;



- 2.6.20 - Permite verificar drives de rede conectados na máquina virtual se necessário;
- 2.6.21 - Capacidade de excluir drives de rede do escopo de proteção;
- 2.6.22 - Suporta Vmware vMotion, se uma máquina é transferida de um ESXi para outro a proteção não é interrompida;
- 2.6.23 - Cria backup de arquivos deletados pela proteção;
- 2.6.24 - Componente dedicado para integração centralizada com o ambiente virtual para evitar carga no Vmware vCenter e impedir chamadas de soluções de antivírus;
- 2.6.25 - Suporte para ativar o software utilizando um código sob subscrição;
- 2.6.26 - Providencia informações sobre números de objetos verificados;
- 2.6.27 - Providencia informações sobre detalhes da definição de antivírus;
- 2.6.28 - Suporta verificação de certificados SSL para comunicação entre o mecanismo de antivírus, servidor de gerenciamento e Componentes de infraestrutura do VMware ;
- 2.6.29 - Importa ou exporta a lista de exclusões e verificações nas tarefas de verificação e perfis de proteção.

2.7 - Requerimentos para antivírus em ambientes virtualizados baseado em agente (conector);

- 2.7.1 - Deve suportar os seguintes Hipervisores:
 - 2.7.1.1 - Vmware ESXi 5.5 com os últimos updates;
 - 2.7.1.2 - Vmware ESXi 6.0 com os últimos updates;
 - 2.7.1.3 - Microsoft Windows Server 2012 R2 Hyper-V (no modo instalação completa ou modo core) com todos os updates disponíveis;
 - 2.7.1.4 - Citrix XenServer 6.5 SP1;
 - 2.7.1.5 - Citrix XenServer 6.2 SP1;
 - 2.7.1.6 - KVM (Kernel-based Virtual Machine) executando sistema operacional Ubuntu Server 14.04 LTS ou CentOS 7;
- 2.7.2 - O Antivírus baseado em agente deve prover proteção para as máquinas virtuais no Vmware hypervisor nos seguintes sistemas operacionais para Desktop:
 - 2.7.2.1 - Microsoft Windows 7 Enterprise x86/x64;
 - 2.7.2.2 - Microsoft Windows 7 Professional SP1 x86/x64;
 - 2.7.2.3 - Microsoft Windows 8.1 Pro/Enterprise x86/x64;
 - 2.7.2.4 - Windows 10 Pro/Enterprise x86/x64;



- 2.7.3 - O Antivirus baseado em agente deve prover proteção para máquinas virtuais no Vmware Hypervisor com os seguintes sistemas operacionais para servidores:
- 2.7.3.1 - Windows Server 2012 R2 (X64);
 - 2.7.3.2 - Windows Server 2012 (x64);
 - 2.7.3.3 - Windows Server 2008 R2 standard SP1 (x64);
- 2.7.4 - O Antivirus baseado em agente deve prover proteção para máquinas virtuais no Microsoft Hyper-V Hypervisor com os seguintes sistemas operacionais para Desktop;
- 2.7.4.1 - Microsoft Windows 7 Enterprise x86/x64;
 - 2.7.4.2 - Microsoft Windows 7 Professional SP1 x86/x64;
 - 2.7.4.3 - Microsoft Windows 8.1 Pro/Enterprise x86/x64;
 - 2.7.4.4 - Windows 10 Pro/Enterprise x86/x64
- 2.7.5 - O antivírus baseado em agente deve prover proteção para máquinas virtuais no Microsoft Hyper-V Hypervisor com os seguintes sistemas operacionais para Servidores;
- 2.7.5.1 - Windows Server 2012 R2 x64;
 - 2.7.5.2 - Windows Server 2012 x64;
 - 2.7.5.3 - Windows Server 2008 R2 Standard SP1 x64;
- 2.7.6 - O antivírus baseado em agente deve prover proteção para máquinas virtuais no Citrix Hypervisor com o seguintes sistemas operacionais para Desktop:
- 2.7.6.1 - Microsoft Windows 7 Enterprise x86/x64;
 - 2.7.6.2 - Microsoft Windows 7 Professional SP1 x86/x64;
 - 2.7.6.3 - Microsoft Windows 8.1 Pro/Enterprise x86/x64;
 - 2.7.6.4 - Microsoft Windows 10 Pro/Enterprise x86/x64;
- 2.7.7 - O antivírus baseado em agente deve prover proteção para máquinas virtuais no Citrix Hypervisor com os seguintes sistemas operacionais para Servidores;
- 2.7.7.1 - Windows Server 2012 R2 x64;
 - 2.7.7.2 - Windows Server 2012 x64;
 - 2.7.7.3 - Windows Server 2008 R2 Standard SP1 x64.
 - 2.7.7.3.1 - O antivírus baseado em agente deve ser compatível com as soluções usadas para criar e gerenciar um a infraestrutura de máquinas virtuais VDI:
 - 2.7.7.3.1.1 - Citrix Provisioning Services 7.1;
 - 2.7.7.3.1.2 - Citrix XenDesktop 7.5



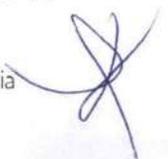
- 2.7.8 - O antivírus baseado em agente deve prover proteção para máquinas virtuais no KVM Hypervisor com os seguintes sistemas operacionais Linux:
- 2.7.8.1 - Ubuntu Server 14.04 LTS;
 - 2.7.8.2 - CentOS 7;
- 2.7.9 - O Antivírus baseado em agente deve prover proteção para máquinas virtuais no KVM com os seguintes sistemas operacionais para servidores:
- 2.7.9.1 - Windows Server 2012 R2 x64;
 - 2.7.9.2 - Windows Server 2012 x64;
 - 2.7.9.3 - Windows Server 2008 R2 Standard SP1 x64;
 - 2.7.9.4 - Ubuntu Server 14.04 LTS;
 - 2.7.9.5 - CentOS 7;

2.8 - O antivírus baseado em agente deve prover as seguintes funcionalidades:

- 2.8.1 - Antivírus e monitoramento residente;
- 2.8.2 - Proteção contra rootkits e auto dialers a sites pagos;
- 2.8.3 - Verificação por heurística para detectar e bloquear malwares desconhecidos;
- 2.8.4 - Transfere a verificação de malware e as tarefas intensivas para uma única máquina virtual responsável pela proteção;
- 2.8.5 - Garante continuidade da proteção de arquivos durante pequenas indisponibilidades na máquina de proteção logando todas as operações de arquivos nas máquinas protegidas durante o período de indisponibilidade, e faz a verificação automática de todas alterações após a restauração do acesso;
- 2.8.6 - Proteção baseada em nuvem contra ameaças novas, permitindo a aplicação acessar recursos especializados da fabricante para obter vereditos durante a verificação em tempo real ou agendada;
- 2.8.7 - Proteção de e-mail contra malwares verificando tráfego de entrada e saída nos protocolos IMAP, SMTP, POP3, MAPI e NNTP independente do cliente de e-mail;
- 2.8.8 - Proteção de tráfego Web: verificação de objetos enviados para os computadores dos usuários via HTTP e FTP, com a possibilidade de adicionar sites confiáveis;
- 2.8.9 - Bloqueia banners e pop-ups nas páginas web;
- 2.8.10 - Capacidade de detectar e bloquear sites de phishing;
- 2.8.11 - Fazer verificação do tráfego de ICQ e MSN para garantir a segurança dos mensageiros;



- 2.8.12 - Proteção contra ameaças não conhecidas baseadas no comportamento;
- 2.8.13 - Capacidade de determinar comportamento anômalo de uma aplicação analisando a sequência de execução.
- 2.8.14 - Capacidade de reverter operações de malware durante o tratamento do arquivo;
- 2.8.15 - Capacidade de restringir o privilégio de programas executáveis tal como escrita no registro ou acesso a arquivos e pastas. Detecção automática de nível de detecção baseado na reputação do programa;
- 2.8.16 - Possuir Firewall que permite criação de regras para pacotes de rede em protocolos específicos (TCP, UDP) e portas;
- 2.8.17 - Permitir criação de regras de rede para programas específicos;
- 2.8.18 - Proteger contra ataques de hackers utilizando o firewall com IDS/IPS e regras de atividade de rede para as aplicações mais conhecidas;
- 2.8.19 - Capacidade de criar regras especiais para bloquear a instalação e/ou execução de uma aplicação. Deve ter a capacidade de controlar a aplicação utilizando o caminho, metadado, MD5, checksum, e categorias predefinidas de aplicações providenciadas pelo fabricante;
- 2.8.20 - Capacidade de monitorar atividade de I/O do usuário na utilização de dispositivos externos pelo tipo de dispositivo e/ou BUS usado incluindo a capacidade de criar uma lista de dispositivos confiáveis através do ID;
- 2.8.21 - Capacidade de garantir privilégios na utilização de dispositivos externos para usuários específicos do AD;
- 2.8.22 - Atualizações centralizadas permitindo que parte do banco de dados de definições seja armazenado na máquina de proteção (SVM);
- 2.8.23 - Habilidade de executar tarefas de detecção de vulnerabilidades em aplicações instaladas nos computadores incluindo opção de submeter um relatório de qualquer vulnerabilidade encontrada;
- 2.8.24 - Integração com o Windows Update para instalar patches de acordo com as vulnerabilidades encontradas;
- 2.8.25 - Capacidade de instalar e distribuir remotamente componentes do antivírus em todas as máquinas protegidas sem utilização de ferramentas de terceiros;
- 2.8.26 - Armazena informações de arquivos verificados para evitar um novo scan sobre o arquivo e aumentar consumo de recursos;
- 2.8.27 - Bloqueia, neutraliza e remove malwares com a opção de notificar os administradores;



2.8.28 - Deve fornecer informações detalhadas sobre os eventos e execução de tarefas;

2.8.29 - Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;

2.8.30 - Capacidade de salvar backup dos arquivos deletados;

2.9 - Suportar as seguintes tecnologias VMware: vMotion, Distributed resource Scheduler;

2.10 - Suportar as seguintes tecnologias Citrix: Virtual User Drive, Citrix Receiver, Multi-stream ICA, XenMotion Live Migration, Automated VM protection and recovery, Dynamic memory control;

2.11 - Suportar as seguintes tecnologias Hyper-V: Live migration, Cluster shared volumes, Dynamic memory, Live backup;

2.12 - Suportar rollback do banco de dados de definições;

2.13 - Requerimentos para administração centralizada, monitoramento e update do software:

2.13.1 - A administração centralizada, monitoramento e atualização de softwares deve funcionar em computadores executando os seguintes sistemas operacionais:

2.13.1.1 - Microsoft Windows 7 Professional/Enterprise/Ultimate/

2.13.1.2 - Microsoft Windows 7 Professional/Enterprise/Ultimate x64;

2.13.1.3 - Microsoft Windows 8 (todas edições);

2.13.1.4 - Microsoft Windows 8 x64 (todas edições);

2.13.1.5 - Microsoft Windows Small Business Server 2008;

2.13.1.6 - Microsoft Windows Small Business Server 2011;

2.13.1.7 - Microsoft Windows Server 2008;

2.13.1.8 - Microsoft Windows Server 2008 instalado no modo servidor core;

2.13.1.9 - Microsoft Windows Server 2008 x64 Service Pack 1 ou posterior;

2.13.1.10 - Microsoft Windows Server 2008 x64 instalado no modo servidor core;

2.13.1.11 - Microsoft Windows Server 2008 R2;

2.13.1.12 - Microsoft Windows Server 2008 R2 implementado no modo core;

2.13.1.13 - Microsoft Windows Server 2012 (Todas edições);

2.13.1.14 - Microsoft Windows Server 2012 implementado no modo core;

2.13.1.15 - Microsoft Windows Server 2016

2.14 - A console de administração centralizada deve suportar os seguintes Bancos de Dados:



- 2.14.1 - Microsoft SQL Server Express 2005;
- 2.14.2 - Microsoft SQL Server Express 2008;
- 2.14.3 - Microsoft SQL Server Express 2008 R2;
- 2.14.4 - Microsoft SQL Server Express 2008 R2 Service Pack 2;
- 2.14.5 - Microsoft SQL Server 2005;
- 2.14.6 - Microsoft SQL Server 2008;
- 2.14.7 - Microsoft SQL Server 2008 R2;
- 2.14.8 - Microsoft SQL Server 2012;
- 2.14.9 - MySQL Enterprise versions 5.0.67, 5.0.77, 5.0.85, 5.0.87 Service Pack 1, 5.0.91;
- 2.14.10 - MySQL Enterprise versions 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90;

2.15 - A console de administração deve suportar os seguintes ambientes virtualizados:

- 2.15.1 - VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5;
- 2.15.2 - Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2
- 2.15.3 - KVM integrado com: RHEL 5.4, 5.x or superior, SLES 11 SPx, Ubuntu 10.10 LTS;
- 2.15.4 - Microsoft Virtual PC 6.0.156.0;
- 2.15.5 - Parallels Desktop 7 ou superior;
- 2.15.6 - CitrixXenServer 5.6.1 FP1 ou superior;
- 2.15.7 - Oracle VM VirtualBox 4.0.4-70112

2.16 - A console de administração centralizada deve prover as seguintes funcionalidades:

- 2.16.1 - Instalação do antivírus a partir de uma única distribuição;
- 2.16.2 - Seleção de instalação dependendo do número de pontos protegidos;
- 2.16.3 - Capacidade de ler informações do AD para obter dados sobre as contas dos computadores na organização;
- 2.16.4 - Capacidade de fazer instalação automática através dos grupos gerenciados;
- 2.16.5 - Capacidade de realocar computadores de acordo com endereço IP, tipo do sistema operacional e localização no AD;
- 2.16.6 - Instalação centralizada;
- 2.16.7 - Remoção centralizada (manual ou automática) de aplicações incompatíveis através do servidor de administração;



- 2.16.8 - Capacidade de instalar o antivírus de diferentes formas: RPC, GPO, agente de administração;
- 2.16.9 - Capacidade de atualizar pacotes de instalação com as últimas atualizações;
- 2.16.10 - Atualizar de forma automática a versão do antivírus e as definições;
- 2.16.11 - Procurar automaticamente por vulnerabilidades nas aplicações e sistemas operacionais presentes da rede;
- 2.16.12 - Capacidade de proibir instalação/execução de aplicações;
- 2.16.13 - Capacidade de gerenciar I/O de dispositivos externos;
- 2.16.14 - Gerenciar a atividade do usuário na internet;
- 2.16.15 - Capacidade de executar instalações automáticas baseado no sistema de proteção dedicado, tais como: VMware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization ou hypervisor;
- 2.16.16 - Criar hierarquia dos servidores de administração e tem capacidade de gerenciar cada um deles através de uma única console de gerenciamento;
- 2.16.17 - Capacidade de criar servidores de administração lógicos, sem a necessidade de ter um servidor adicional para gerenciamento;
- 2.16.18 - Distribuir automaticamente licenças nos computadores gerenciados;
- 2.16.19 - Criar inventário de software e hardware dos computadores gerenciados na rede;
- 2.16.20 - Instalação centralizada de aplicações de terceiros;
- 2.16.21 - Capacidade de eleger um computador na rede para ser responsável por atualizar outros computadores dentro da rede;
- 2.16.22 - Capacidade de gerar relatórios gráficos;
- 2.16.23 - Capacidade de exportar relatórios para PDF, XML e CSV;
- 2.16.24 - Capacidade de criar contas internas para autenticar na console de administração;
- 2.16.25 - Capacidade de criar backup de forma automática ou manual;
- 2.16.26 - Suporta Windows Failover Clustering;
- 2.16.27 - Console WEB para gerenciar a aplicação;
- 2.16.28 - Sistema para controle de virus outbreak.
- 2.16.29 - Capacidade de gerenciar permissões de administradores;
- 2.16.30 - Capacidade de gerenciar dispositivos móveis remotamente;
- 2.16.31 - Capacidade de deletar atualizações já baixadas;
- 2.16.32 - Capacidade de distribuir correções de vulnerabilidades em computadores clientes sem instalar atualizações.



QUANTIDADE: 50 (CINQUENTA) LICENÇAS

VALOR UNITÁRIO R\$ 320,32 (TREZENTOS E VINTE REAIS E TRINTA E DOIS CENTAVOS)

VALOR TOTAL R\$ 16.016,00 (DEZESSEIS MIL E DEZESSEIS REAIS)

VALOR TOTAL (Item 01 + Item 02) R\$64.900,00 (SESSENTA E QUATRO MIL E NOVECENTOS REAIS)



SAF - DEPARTAMENTO DE CONTRATOS E CONVÊNIOS

FORNECIMENTO/AQUISIÇÃO

EXTRATO DE CONTRATO

| | |
|----------------------|--|
| CONTRATO Nº 005/2018 | |
| CONTRATANTE | ASSEMBLÉIA LEGISLATIVA DA BAHIA |
| C.N.P.J. | 14.674.337/0001-99 |
| CONTRATADA | VTECH COMÉRCIO SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA EIRELI - EPP |
| C.N.P.J. | 22.122.370/0001-34 |
| OBJETO | AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA ANTIVÍRUS PARA ESTAÇÕES DE TRABALHO, MÁQUINAS SERVIDORES E MÁQUINAS SERVIDORES VIRTUAIS. |
| VALOR | R\$ 64.900,00 (SESSENTA E QUATRO MIL E NOVECENTOS REAIS) |
| PROCESSO Nº | Nº 2018000236 |
| LICITAÇÃO | PREGÃO Nº 006/2018 |
| VIGÊNCIA | 12 (DOZE) MESES - A PARTIR DA DATA DE ASSINATURA - 21/03/2018 À 20/03/2019 |
| DOTAÇÃO ORÇAMENTÁRIA | |
| ATIVIDADE | 7167 |
| ELEMENTO | 3390.39 |

PRESTAÇÃO DE SERVIÇOS

EXTRATO DE ADITAMENTO

| | |
|--------------|--|
| CONTRATO Nº: | 041/2017. |
| CONTRATADA: | CLAND CONSTRUÇÃO E LOCAÇÃO LTDA - ME |
| VALOR: | ADITAR O CONTRATO EM TORNO DE 50% (CINQUENTA POR CENTO), CORRESPONDENDO AO ACRÉSCIMO, NO VALOR DE R\$ 115.468,80 (CENTO E QUINZE MIL, QUATROCENTOS E SESSENTA OITO REAIS E OITENTA CENTAVOS), PERFAZENDO O VALOR TOTAL DE R\$ 346.406,46 (TREZENTOS E QUARENTA E SEIS MIL, QUATROCENTOS E SEIS REAIS E QUARENTA E SEIS CENTAVOS), A FIM DE ATENDER A NECESSIDADE DA CASA, CONSTANTE DO ANEXO I, CONFORME PROCESSO Nº 2018001462. |

EXTRATO DE CONTRATO

| | |
|----------------------|---|
| CONTRATO Nº 004/2018 | |
| CONTRATANTE | ASSEMBLÉIA LEGISLATIVA DA BAHIA |
| C.N.P.J. | 14.674.337/0001-99 |
| CONTRATADA | KENTA INFORMÁTICA S.A |
| C.N.P.J. | 01.276.330/0001 - 77 |
| ENDEREÇO | RUA RIACHUELO, 1098 - CENTRO - PORTO ALEGRE- RS. |
| OBJETO | PRESTAÇÃO DE SERVIÇOS DE SUPORTE TÉCNICO E ATUALIZAÇÃO DE VERSÕES PARA 37 LICENÇAS DE USO DRS PLENÁRIO LIMITED, O SISTEMA PSS - PROCESS & STORAGE SOUND, NO ÂMBITO DA ASSEMBLEIA LEGISLATIVA DA BAHIA, COM CAPTURA DO ÁUDIO DAS SESSÕES, GRAVAÇÃO DIGITAL, ARMAZENAMENTO, GERENCIAMENTO E DISPONIBILIZAÇÃO DESTAS INFORMAÇÕES |

| | |
|----------------------|--|
| VALOR | R\$ 3.312,98 (TRÊS MIL TREZENTOS E DOZE REAIS E NOVENTA E OITO CENTAVOS) ESTIMADO MENSAL, PERFAZENDO O VALOR ESTIMADO ANUAL DE R\$ 39.755,76 (TRINTA E NOVE MIL SETECENTOS E CINQUENTA E CINCO REAIS E SETENTA E SEIS CENTAVOS). |
| PROCESSO Nº | Nº 2018001221. |
| LICITAÇÃO | INEXIGIBILIDADE Nº 004/2018 |
| VIGÊNCIA | 12 (DOZE) MESES - A PARTIR DA DATA DE ASSINATURA - 21/03/2018 À 20/03/2019 |
| DOTAÇÃO ORÇAMENTÁRIA | |
| ATIVIDADE | 2000 |
| ELEMENTO | 3390.39 |

EXTRATO DE CONTRATO

| | |
|----------------------|---|
| CONTRATO Nº 003/2018 | |
| CONTRATANTE | ASSEMBLÉIA LEGISLATIVA DA BAHIA |
| C.N.P.J. | 14.674.337/0001-99 |
| CONTRATADA | RELEVO CONSTRUTORA LTDA - ME |
| C.N.P.J. | 09.102.297/0001-70 |
| ENDEREÇO | RUA WALTER JOSÉ TOLENTINO ALVES, 130 EDF. MULTICENTER, SALA 118, CENTRO, SIMOES FILHO - BAHIA. |
| OBJETO | CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM ENGENHARIA PARA SUBSTITUIÇÃO DA ESTRUTURA METÁLICA DA PELE DE VIDRO E DO TELHADO ENTRE PREDIOS NESLSON DAVID E WILSON LINS, DA ALBA, CONFORME ESPECIFICADOS NO ANEXO I. |
| VALOR | R\$ 161.405,84 (CENTO E SESSENTA E UM MIL QUATROCENTOS E CINCO REAIS E OITENTA E QUATRO CENTAVOS) ESTIMATIVO GLOBAL. |
| PROCESSO Nº | Nº 2018000348 |
| LICITAÇÃO | TOMADA DE PREÇOS Nº 001/2018 |
| VIGÊNCIA | 12 (DOZE) MESES - A PARTIR DA DATA DE ASSINATURA - 26/03/2018 À 25/03/2019 |
| DOTAÇÃO ORÇAMENTÁRIA | |
| ATIVIDADE | 7166 |
| ELEMENTO | 3390.39 |

Certificação Digital

Garante a autenticidade e não-repúdio nas transações eletrônicas.

Contato:
71 3116-2137

egba

IMPRENSA OFICIAL

www.egba.ba.gov.br