ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

CONTRATO Nº 05/2018

CONTRATO QUE ENTRE SI CELEBRAM O ESTADO DA BAHIA E A VTECH COMERCIO SERVICOS E EQUIPAMENTOS DE INFORMATICA, PARA OS FINS QUE NELE SE DECLARAM.

O **ESTADO DA BAHIA,** neste ato representado pelo **DR. PAULO MORENO CARVALHO,** titular da **PROCURADORIA GERAL DO ESTADO,** CNPJ nº 04.139.403/0001-77, situada na 3º. Avenida, 370, Centro Administrativo da Bahia, CEP: 41.745-005 autorizado pelo Decreto de delegação de competência publicado no D.O.E. de 07/01/2015, doravante denominado **CONTRATANTE,** e a **VTECH COMERCIO SERVICOS E EQUIPAMENTOS DE INFORMATICA,** CNPJ n nº 22.122.370/0001-34, Inscrição Estadual nº 123.555.216 EPP, situada na Avenida Santos Dumont, 4487, Km 3,5, Loja 157, Shopping Passeio Norte, Estrada do Coco, em Lauro de Freitas, Estado da Bahia, CEP 42700-000, neste ato representada pela **SR. LUCIANA SANTOS DA SILVA,** portador da cédula de identidade no 668313188, emitida por SSP-BA, inscrito no CPF/MF sob o no 790.641.595-72 , adjudicatária do pregão nº 016/2018, processo administrativo nº 006.0409.2018.0001444-39, doravante denominada **CONTRATADA,** celebram o presente contrato, que se regerá pela Lei estadual nº 9.433/05, pelas normas gerais da Lei nº 8.666/93, e respectivas alterações, bem como pela legislação específica, mediante as cláusulas e condições a seguir ajustadas:

CLÁUSULA PRIMEIRA – OBJETO

Constitui objeto do presente contrato a prestação de serviços de licenças de software antivírus para estações de trabalho e servidores em console de gerenciamento, contendo serviço de instalação, configuração e suporte on-site, com garantia de 36 (trinta e seis) meses, de acordo com as especificações do Termo de Referência do instrumento convocatório e da proposta apresentada pela CONTRATADA, que integram este instrumento na qualidade de Anexos I e II, respectivamente.

§1º A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem no objeto, de até 25% do valor inicial atualizado do contrato, na forma dos §1º e 2º do art. 143 da Lei estadual nº 9.433/05.

§2º As supressões poderão ser superiores a 25%, desde que haja resultado de acordo entre os contratantes.

§3º É vedada a subcontratação parcial do objeto, a associação da CONTRATADA com outrem, a cessão ou transferência, total ou parcial do contrato, não se responsabilizando o CONTRATANTE por nenhum compromisso assumido por aquela com terceiros.

CLÁUSULA SEGUNDA – PRAZO

[SERVIÇOS NÃO-CONTÍNUOS]

O prazo de vigência do contrato, a contar da data (x) da sua assinatura do contrato, será de 36 (trinta e seis) meses, admitindo-se a sua prorrogação exclusivamente nos termos do art. 141 da Lei estadual nº 9.433/05.

§1º A prorrogação do prazo de vigência está condicionada à ocorrência de, ao menos, uma das hipóteses do art. 141 da Lei estadual nº 9.433/05.

§2º A prorrogação deverá ser previamente justificada e autorizada pela autoridade competente para celebrar o ajuste e será realizada por meio de termo aditivo, antes do termo final do contrato.

CLÁUSULA TERCEIRA – GARANTIA

(x) Não exigível

CLÁUSULA QUARTA – REGIME DE EXECUÇÃO

(**x**) **Serviço** com empreitada por preço ( ) global (x) unitário

CLÁUSULA QUINTA – PREÇO

O CONTRATANTE pagará à CONTRATADA pelos serviços efetivamente prestados, os valores abaixo especificados:

LOTE I						
ITEM	**Código SIMPAS**	**Descrição**	**Unidade de Fornecimento (UF)**	**Quantitativo**	**PREÇO UNITÁRIO**	**PREÇO MENSAL**
1	02.26.17.00000656-4	**Fornecimento de licença de Software antivírus, Kaspersky Security for Business ADVANCED para estações de trabalho e servidores com console de gerenciamento, contando serviço de instalação, configuração e suporte on-site. Com garantia de 36 (trinta e seis) meses. (Marca/Modelo: Kaspersky Security for Business ADVANCED, Fabricante: Kaspersky, Procedência Russa.**	UN	1000	R$ 99,60	R$ 99.600,00
				VALOR ESTIMADO GLOBAL		R$ 99.600,00

§1º Estima-se para o contrato o valor global de R$ 99.600,00 (Noventa e nove mil e seiscentos reais)

§2º Nos preços contratados estão incluídos todos os custos com material de consumo, salários, encargos sociais, previdenciários e trabalhistas de todo o pessoal da CONTRATADA, como também fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela CONTRATADA das obrigações. **[NOTA: Excepcionar esta cláusula, quando algum tipo fornecimento for de responsabilidade do CONTRATANTE]**

CLÁUSULA SEXTA – DOTAÇÃO ORÇAMENTÁRIA

As despesas para o pagamento deste contrato correrão por conta dos recursos da Dotação Orçamentária a seguir especificada:

Unidade FIPLAN	Função	Subfunção	Programa	P/A/OE
06601	03	126	218	7033
Região/planejamento	**Natureza da despesa**	**Destinação do recurso**	**Tipo de recurso orçamentário**	
7800	339039	154	Normal	

CLÁUSULA SÉTIMA – OBRIGAÇÕES DA CONTRATADA

A CONTRATADA, além das determinações contidas no Termo de Referência do Instrumento convocatório, bem como daquelas decorrentes de lei, obriga-se a:

I. designar de sua estrutura administrativa um preposto permanentemente responsável pela perfeita execução dos serviços, inclusive para atendimento de emergência;
II. executar os serviços objeto deste contrato de acordo com as especificações técnicas constantes do Instrumento convocatório e do presente contrato, nos locais, dias, turnos e horários determinados;
III. manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e recursos humanos para execução completa e eficiente dos serviços objeto deste contrato;

IV. zelar pela boa e completa execução dos serviços contratados e facilitar, por todos os meios ao seu alcance, a ampla ação fiscalizadora dos prepostos designados pelo CONTRATANTE, atendendo prontamente às observações e exigências que lhe forem solicitadas;

V. comunicar ao CONTRATANTE qualquer anormalidade que interfira no bom andamento dos serviços;

VI. atender com presteza as reclamações sobre a qualidade dos serviços executados, providenciando sua imediata correção, sem ônus para o CONTRATANTE;

VII. respeitar e fazer com que seus empregados respeitem as normas de segurança do trabalho, disciplina e demais regulamentos vigentes no CONTRATANTE, bem como atentar para as regras de cortesia no local onde serão executados os serviços;

VIII. reparar, repor ou restituir, nas mesmas condições e especificações, dentro do prazo que for determinado, os equipamentos e utensílios eventualmente recebidos para uso nos serviços objeto deste contrato, deixando as instalações na mais perfeita condição de funcionamento;

IX. arcar com todo e qualquer dano ou prejuízo de qualquer natureza causado ao CONTRATANTE e terceiros, por sua culpa, ou em conseqüência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir o equivalente a todos os danos decorrentes de paralisação ou interrupção dos serviços contratados, exceto quando isto ocorrer por exigência do CONTRATANTE ou ainda por caso fortuito ou força maior, circunstâncias que deverão ser comunicadas no prazo de 48 (quarenta e oito) horas após a sua ocorrência;

X. manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, inclusive de apresentar, ao setor de liberação de faturas e como condição de pagamento, os documentos necessários;

XI. providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes, necessários à execução dos serviços;

XII. efetuar pontualmente o pagamento de todas as taxas e impostos que incidam ou venham a incidir sobre as suas atividades e/ou sobre a execução do objeto do presente contrato;

XIII. adimplir os fornecimentos exigidos pelo instrumento convocatório e pelos quais se obriga, visando à perfeita execução deste contrato;

XIV. emitir notas fiscais/faturas de acordo com a legislação;

XV. observar a legislação federal, estadual e municipal relativa ao objeto do contrato;

XVI. executar os serviços sem solução de continuidade durante todo o prazo da vigência do contrato.

PARÁGRAFO ÚNICO. Além das determinações acima descritas, a CONTRATADA deverá atender às seguintes obrigações específicas:

a) observar a determinação do art. 429 do Decreto-Lei nº 5.452, de 1º de maio de 1943 (Consolidação das Leis do Trabalho - CLT), regulamentado pelo Decreto nº 5.598, de 1º de dezembro de 2005;

b) recrutar, preferencialmente, para a contratação de aprendizes determinada pelo art. 429 da CLT, os estudantes indicados nos incisos I e II do art. 9º da Lei estadual nº 13.459, de 10 dezembro de 2015, regulamentada pelo Decreto estadual nº 16.761, de 07 de junho de 2016, no percentual mínimo de 20% (vinte por cento) do quadro de aprendizes da CONTRATADA;

c) apresentar ao fiscal ou responsável pela gestão e acompanhamento do contrato, no prazo de até 05 (cinco) dias úteis contado do início efetivo da execução do serviço, a lista completa dos aprendizes, indicando aqueles selecionados no banco de dados de que trata o Decreto estadual nº 16.761/16, devendo justificar, perante o CONTRATANTE, a eventual impossibilidade de seu cumprimento.

d) A CONTRATADA fornecerá, por sua conta, a instalação, configuração e licenças de todos os softwares que se fizerem necessários para a execução contratual da prestação de serviços decorrentes deste contrato.

e) 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.

f) A CONTRATADA não poderá transferir a outrem os compromissos assumidos, no todo ou em parte, os serviços.

CLÁUSULA OITAVA – OBRIGAÇÕES DO CONTRATANTE

O **CONTRATANTE,** além das obrigações contidas neste contrato por determinação legal, obriga-se a:

I. fornecer à CONTRATADA os elementos indispensáveis ao cumprimento do contrato no prazo máximo de 10 (dez) dias da assinatura;

II. realizar o pagamento pela execução do objeto contratual;

III. proceder à publicação resumida do instrumento de contrato e de seus aditamentos, na imprensa oficial, no prazo legal.

CLÁUSULA NONA – FISCALIZAÇÃO DO CONTRATO E RECEBIMENTO DO OBJETO

Competirá ao CONTRATANTE proceder ao acompanhamento da execução do contrato, na forma do art. 154 da Lei estadual nº 9.433/05, ficando esclarecido que a ação ou omissão, total ou parcial da fiscalização não eximirá a CONTRATADA da total responsabilidade pela execução do contrato.

§1º O adimplemento da obrigação contratual por parte da CONTRATADA ocorrerá com a efetiva prestação do serviço, a realização da obra, a entrega do bem ou de parcela destes, bem como qualquer outro evento contratual cuja ocorrência esteja vinculada à emissão de documento de cobrança, nos termos do art. 8º, inc. XXXIV, da Lei estadual nº9.433/05.

§2º Cumprida a obrigação pela CONTRATADA, caberá ao CONTRATANTE proceder ao recebimento do objeto, a fim de aferir os serviços ou fornecimentos efetuados, para efeito de emissão da habilitação de pagamento, conforme o art. 154, inc. V, e art. 155, inc. V, da Lei estadual nº 9.433/05.

§3º O recebimento do objeto se dará segundo o disposto no art. 161 da Lei estadual nº 9.433/05, observando-se os seguintes prazos, se outros não houverem sido fixados no Termo de Referência:

I. se a verificação da conformidade do objeto com a especificação, bem assim do cumprimento das obrigações acessórias puder ser realizada de imediato, será procedido de logo o recebimento definitivo;

II. quando, em razão da natureza, do volume, da extensão, da quantidade ou da complexidade do objeto, não for possível proceder-se a verificação imediata de conformidade, será feito o recebimento provisório, devendo ser procedido ao recebimento definitivo no prazo de 15 (quinze) dias.

§4º O recebimento definitivo de obras, compras ou serviços, cujo valor do objeto seja superior ao limite estabelecido para a modalidade de convite, deverá ser confiado a uma comissão de, no mínimo, 03 (três) membros.

§5º Tratando-se de equipamentos de grande vulto, o recebimento definitivo far-se-á mediante termo circunstanciado e, nos demais, mediante recibo.

§6º Esgotado o prazo total para conclusão do recebimento definitivo sem qualquer manifestação do órgão ou entidade CONTRATANTE, considerar-se-á definitivamente aceito o objeto contratual, para todos os efeitos.

§7º Com a conclusão da etapa do recebimento definitivo, a CONTRATADA estará habilitada a apresentar as nota(s) fiscal(is)/fatura(s) para pagamento.

§8º O CONTRATANTE rejeitará, no todo ou em parte, obra, serviço ou fornecimento em desacordo com as condições pactuadas.

§9º O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança da obra ou do serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo contrato, consoante o art. 165 da Lei estadual nº 9.433/05.

§10 Fica indicada como área gestora do contrato a Coordenação de Gestão Estratégica, bem como fica indicado como fiscal(is) deste Contrato o Servidor: **Mauricio de Cerqueira Pereira Matrícula: 06.579.186-0**

CLÁUSULA DÉCIMA – PAGAMENTO

Os pagamentos devidos à CONTRATADA serão efetuados através de ordem bancária ou crédito em conta corrente, no prazo não superior a 08 (oito) dias úteis, contados da data da apresentação da fatura, após concluído o recebimento definitivo, em consonância com o disposto no art. 6º, §5º; art. 8º, XXXIV; art. 79, XI, "a"; art. 154, V e art. 155, V da Lei estadual nº 9.433/05.

§1º A(s) nota(s) fisca(l)is/fatura(s) somente deverá(ao) ser apresentada(s) para pagamento após a conclusão da etapa do recebimento definitivo, indicativo da satisfação pela CONTRATADA de todas as obrigações pertinentes ao objeto contratado.

§2º Ainda que a nota fiscal/fatura seja apresentada antes do prazo definido para recebimento definitivo, o prazo para pagamento somente fluirá após o efetivo atesto do recebimento definitivo.

§3º O CONTRATANTE descontará da fatura mensal o valor correspondente às faltas ou atrasos no cumprimento da obrigação, com base no valor do preço vigente.

§4º A(s) nota(s) fisca(l)is/fatura(s) deverá(ao) atender as exigências legais pertinentes aos tributos e encargos relacionados com a obrigação e, para efeito do art. 126, inciso XVI, da Lei estadual nº 9.433/05, o processo de pagamento deverá ser instruído com a prova da manutenção das condições de habilitação e qualificação estabelecidas na licitação, considerando-se como marco final a data de conclusão da etapa do recebimento definitivo, cuja demonstração poderá ser aferida mediante consulta ao Registro Cadastral ou a sites oficiais.

§5º 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, de 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 o CONTRATANTE.

§6º As situações previstas na legislação específica sujeitar-se-ão à emissão de nota fiscal eletrônica.

§7º A atualização monetária dos pagamentos devidos pelo CONTRATANTE, 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 *pro rata tempore*.

CLÁUSULA DÉCIMA-PRIMEIRA – MANUTENÇÃO DAS CONDIÇÕES DA PROPOSTA

Os preços contratados são fixos e irreajustáveis durante o prazo de 12 meses da data de apresentação da proposta.

§1º Após o prazo de 12 meses a que se refere o *caput*, a concessão de reajustamento será feita mediante a aplicação do INPC/IBGE, nos termos do inc. XXV do art. 8º da Lei estadual nº 9.433/05.

§2º A revisão de preços, nos termos do inc. XXVI do art. 8º da Lei estadual nº 9.433/05, dependerá de requerimento da CONTRATADA quando visar recompor o preço que se tornou *insuficiente*, devendo ser instruído com a documentação que comprove o desequilíbrio econômico-financeiro do contrato.

§3º O requerimento de revisão de preços deverá ser formulado pela CONTRATADA no prazo máximo de um ano a partir do fato que a ensejou, sob pena de decadência, em consonância com o art. 211 da Lei nº 10.406/02.

§4º A revisão de preços pode ser instaurada pelo CONTRATANTE quando possível a redução do preço ajustado para compatibilizá-lo ao valor de mercado ou quando houver diminuição, devidamente comprovada, dos preços dos insumos básicos utilizados no contrato, conforme o art. 143, inc. II, alínea "e", da Lei estadual nº 9.433/05.

CLÁUSULA DÉCIMA-SEGUNDA – ALTERAÇÕES CONTRATUAIS

A prorrogação, suspensão ou rescisão sujeitar-se-ão às mesmas formalidades exigidas para a validade deste contrato.

§1º A admissão da fusão, cisão ou incorporação da CONTRATADA está condicionada à manutenção das condições de habilitação e à demonstração, perante o CONTRATANTE, da inexistência de comprometimento das condições originariamente pactuadas para a adequada e perfeita execução do contrato.

§2º Independem de termo contratual aditivo, podendo ser registrado por simples apostila:

I. a simples alteração na indicação dos recursos orçamentários ou adicionais custeadores da despesa, sem modificação dos respectivos valores;

II. reajustamento de preços previsto no edital e neste contrato, bem como as atualizações, compensações ou apenações financeiras decorrentes das condições de pagamento dos mesmos constantes;

III. o empenho de dotações orçamentárias suplementares até o limite do seu valor corrigido.

§3º Somente será admitida a substituição de algum membro da equipe técnica, no curso da execução do contrato, por outro profissional de experiência equivalente ou superior, devidamente comprovada, e desde que previamente aprovada pelo CONTRATANTE.

CLÁUSULA DÉCIMA-TERCEIRA - INEXECUÇÃO E RESCISÃO

A inexecução total ou parcial do contrato ensejará a sua rescisão, com as conseqüências contratuais e as previstas na Lei estadual nº 9.433/05.

§1º A rescisão poderá ser determinada por ato unilateral e escrito do CONTRATANTE nos casos enumerados nos incisos I a XV, XX e XXI do art. 167 da Lei estadual nº 9.433/05.

§2º Quando a rescisão ocorrer com base nos incisos I e XVI a XX do art. 167 da Lei estadual nº 9.433/05, sem que haja culpa do contratado, será este ressarcido dos prejuízos regularmente comprovados que houver sofrido, na forma do §2º do art. 168 do mesmo diploma.

CLÁUSULA DÉCIMA-QUARTA – PENALIDADES

Constituem ilícitos administrativos as condutas previstas nos arts. 184, 185 e 199 da Lei estadual nº 9.433/05, sujeitando-se os infratores às cominações legais, especialmente as definidas no art. 186 do mesmo diploma, garantida a prévia e ampla defesa em processo administrativo.

§1º Para a aplicação das penalidades serão levados em conta a natureza e a gravidade da falta, os prejuízos dela advindos para a Administração Pública e a reincidência na prática do ato, observando-se os critérios de dosimetria estabelecidos pelo Decreto estadual nº 13.967/12.

§2º Serão punidos com a pena de declaração de inidoneidade para licitar e contratar com a Administração, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a autoridade competente para aplicar a punição, os que incorram nos ilícitos previstos nos incisos I a V do art. 184, nos incisos II, III e V do art. 185 e no art. 199 da Lei estadual nº 9.433/05.

§3º Serão punidos com a pena de suspensão temporária do direito de cadastrar e licitar e impedimento de contratar com a Administração os que incorram nos ilícitos previstos nos incisos VI e VII do art. 184 e nos incisos I, IV, VI e VII do art. 185 da Lei estadual nº 9.433/05.

§4º A CONTRATADA será descredenciada do Sistema de Registro Cadastral quando, em razão da ocorrência das faltas previstas na Lei estadual nº 9.433/05, deixar de satisfazer as exigências relativas à habilitação jurídica, qualificação técnica, qualificação econômico-financeira, regularidade fiscal e trabalhista exigidas para cadastramento.

§5º A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará a CONTRATADA à multa de mora, na forma prevista na cláusula seguinte, que será graduada de acordo com a gravidade da infração, observado o disposto na Lei estadual nº 9.433/05 e no Decreto estadual nº 13.967/12.

CLÁUSULA DÉCIMA-QUINTA – SANÇÃO DE MULTA

A pena de multa será aplicada em função de inexecução contratual, inclusive por atraso injustificado na execução do contrato, sem prejuízo da rescisão unilateral do contrato, a qualquer tempo, e a aplicação das demais sanções previstas na Lei estadual nº 9.433/05.

§1º Quanto à obrigação principal, será observado o que se segue:

I. Em caso de descumprimento total da obrigação principal, será aplicada multa no percentual 10% (dez por cento) incidente sobre o valor global do contrato.

II. Caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicado o percentual de 10% (dez por cento) sobre o saldo do contrato, isto é, sobre a diferença entre o valor global do contrato e o valor da parte do fornecimento ou do serviço já realizado.

III. O atraso no cumprimento da obrigação principal ensejará a aplicação de multa no percentual de 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, e de 0,7% (sete décimos por cento) por cada dia subseqüente ao trigésimo, calculados sobre o valor da parcela do fornecimento ou do serviço em mora.

§2º Quanto à obrigação acessória, assim considerada aquela que coadjuva a principal, será observado o que se segue:

I. Em caso de descumprimento total da obrigação acessória, será aplicada multa no percentual de 10% (dez por cento) incidente sobre o valor ou custo da obrigação descumprida.

II. Caso o cumprimento da obrigação acessória, uma vez iniciado, seja descontinuado, será aplicado o percentual de 5% (cinco por cento) sobre o valor ou custo da obrigação descumprida.

III. O atraso no cumprimento da obrigação acessória ensejará a aplicação de multa no percentual de 0,2% (dois décimos por cento) ao dia, até o trigésimo dia de atraso, e de 0,6% (seis décimos por cento) por cada dia subseqüente ao trigésimo, calculados sobre o valor ou custo da obrigação descumprida.

§3º Se a multa moratória atingir o patamar de 10% (dez por cento) do valor global do contrato, deverá, salvo justificativa escrita devidamente fundamentada, ser recusado o recebimento do objeto, sem prejuízo da aplicação das demais sanções previstas em lei.

§4º Na hipótese de o contratado se negar a efetuar o reforço da caução, dentro de 10 (dez) dias contados da data de sua convocação, será aplicada multa no percentual de 2,5% (dois e meio por cento) incidente sobre o valor global do contrato.

§5º As multas previstas nesta cláusula não têm caráter compensatório e o seu pagamento não eximirá a CONTRATADA da responsabilidade por perdas e danos decorrentes das infrações cometidas.

§6º A multa, aplicada após regular processo administrativo, será descontada da garantia do contratado faltoso.

§7º Se o valor da multa exceder ao da garantia prestada, além da perda desta, a CONTRATADA responderá pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou, ainda, se for o caso, cobrada judicialmente.

§8º Caso não tenha sido exigida garantia, à Administração se reserva o direito de descontar diretamente do pagamento devido à CONTRATADA o valor de qualquer multa porventura imposta.

CLÁUSULA DÉCIMA-SEXTA - DA PROPRIEDADE INTELECTUAL

A Contratada entregará a Contratante toda e qualquer documentação gerada em função da prestação de serviços decorrente deste contrato. A Contratada concordará que os direitos patrimoniais autorais relativos aos resultados produzidos durante a vigência do Contrato são de propriedade exclusiva da Contratante, devidamente amparada pela Lei nº 9.610/1998, de Diretos 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.

§1º A Contratada fica 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 DÉCIMA-SÉTIMA – DA ENTREGA, DO ACEITE E DA INSTALAÇÃO

§1º A entrega e instalação do software será feita de acordo com plano de implantação apresentado pela Contratada e aprovado pela Contratante;

§2º A instalação deverá seguir cronograma previsto no plano de implantação;

§3º O aceite definitivo será dado pela PGE, após a implantação e entrada em operação do software fornecido;

§4º O aceite do software será feito mediante emissão pela "Comissão de Recebimento", nomeada pela PGE, do "Termo de Recebimento e Aceitação";

§5º Como parte dos documentos de aceite do software fornecido, a CONTRATADA deverá apresentar "Tabela de Comprovação Técnica" das especificações exigidas neste Termo de Referência (apresentar na Tabela a correlação das especificações com a respectiva comprovação técnica, exemplo, página, item, documento, etc.). A comprovação técnica deverá ser efetuada através de documentos oficiais referentes ao produto fornecido, bem como referente aos módulos complementares.

CLÁUSULA DÉCIMA-OITAVA - VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO

Integra o presente contrato, como se nele estivessem transcritas, as cláusulas e condições estabelecidas no processo licitatório referido no preâmbulo deste instrumento e na proposta da licitante vencedora.

CLÁUSULA DÉCIMA-NONA – FORO

As partes elegem o Foro da Cidade do Salvador, Estado da Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas oriundas deste contrato.

E, por estarem assim justos e contratados, firmam o presente contrato em 02 (duas) vias de igual teor e forma na presença das testemunhas que subscrevem depois de lido e achado conforme.

Salvador, 17 de janeiro de 2019.

CONTRATANTE

CONTRATADA

Testemunha (nome/CPF)

Coordenadora IV
Cad.: 06.576.4

Testemunha (nome/CPF)

Coordenadora IV

ANEXO I

SEÇÃO II
TERMO DE REFERÊNCIA DO OBJETO DA LICITAÇÃO

1. Descritivo: a presente licitação tem por objeto a contratação de Licenças de Software Antivírus para estações de trabalho e servidores em console de gerenciamento, contendo serviço de instalação, configuração e suporte on-site, com garantia de 36 (trinta) e seis meses.

2. Especificações, características, quantitativos, cronograma/prazo de execução e local da prestação dos serviços:

LOTE ÚNICO				
ITEM	**Descrição**	**Unidade de Fornecimento (UF)**	**Quantitativo**	**Cronograma/Prazo**
1	LICENÇA DE SOFTWARE, antivírus, contendo: Gerenciamento de licenças, inventário de hardware, instalação de software, imagens e provisionamento, gerenciamento de correções e verificação de vulnerabilidades, criptografia de arquivos e pastas, controle de aplicativos, controle de dispositivos e controle WEB; Para estações de trabalho Windows, Linux, Mac, dispositivos móveis e servidores com console de gerenciamento; com instalação, manutenção, suporte e treinamento. Código SIMPAS: 02.26.17.00000656-4	UN	1.000	Prazo de entrega: até 30 (trinta) dias, contados a partir da assinatura do contrato ou instrumento equivalente; Período do licenciamento: 36 (trinta e seis) meses

2.1 Local da prestação de serviço: Os serviços serão prestados na Sede da Procuradoria Geral do Estado, situada na 3ª Avenida, 370, Centro Administrativo da Bahia, CEP: 41.745-005, Salvador/BA.

2.2 Especificações gerais:

2.2.1 O objeto descrito neste Termo de Referência deverá ser entregue e instalado pelos técnicos da empresa fornecedora, na quantidade e características especificadas e dentro do prazo fixado e respeitando os termos estabelecidos neste edital;

2.2.2 O produto deverá estar licenciado em nome da PGE, sendo que o suporte, a manutenção e suas atualizações (*upgrade* e *update*) deverão ocorrer sem ônus para este Órgão;

2.2.3 O período de licenciamento do software será de 36 (trinta e seis) meses, com suporte técnico de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, na cidade de Salvador (BA). Durante o período de licenciamento o fabricante val garantir o funcionamento do software, com suporte técnico prestado em caso de falha. Deverá ser garantida neste prazo a atualização de versões, releases, componentes (bibliotecas, filtros, etc.) e módulos dos produtos. Todos os produtos deverão ter o mesmo período de licenciamento.

2.2.4 Acesso telefônico 08h/dia, 5 dias da semana;

2.2.5 Treinamento hands-on para pelo menos 05 (cinco) técnicos nas instalações da Contratante;

2.2.6 Suporte técnico ao produto fornecido em língua portuguesa

2.3 DO SUPORTE TÉCNICO

2.3.1 O suporte técnico ao produto fornecido deverá ser prestado pelo através de contato Telefônico (telefone 0800 do fabricante ou telefone com numeração comum do fornecedor), Sitio de Internet (website do fabricante ou do fornecedor), Correio Eletrônico (e-mail do fabricante ou do fornecedor) ou no Local (provido pelo fabricante ou pelo fornecedor), em casos de grande emergência;

2.3.2 O suporte técnico deverá ser fornecido prioritariamente pelo fornecedor da solução de segurança ou pelo fabricante, no Brasil e na língua portuguesa;

2.3.3 Deverão ser executados pela empresa contratada serviços de Consultoria, Instalação e Configuração para uso da solução contratada com supervisão da equipe técnica da PGE;

2.3.4 Deverá ser executada pela empresa contratada uma análise da situação atual e elaborar, em conjunto com a equipe interna da PGE, um plano de otimização de recursos, rotinas, procedimentos e processos para o novo ambiente de segurança. Essa documentação deverá ser entregue, pela empresa contratada, em formato digital;

2.3.5 A empresa contratada deverá preservar todo ambiente computacional existente, de forma a manter a integridade dos dados, aplicativos e sistemas operacionais em funcionamento;

2.3.6A empresa contratada deverá preparar o ambiente de modo a operar conforme o estabelecido no plano de otimização de recursos, rotinas, procedimentos e processos;

2.3.7 A instalação e configuração da solução deverá ser realizada de acordo com o horário de funcionamento da PGE, de segunda à sexta-feira, das 8:30 às 18:00h, em horário e dias a serem combinados entre o PGE e a contratada;

2.3.8 A instalação e configuração dos softwares adquiridos deverão ser executadas em 100% do Parque PGE, localizado em Salvador (BA);

2.3.9 Deverá ser oferecido treinamento ou hands-on para a solução implantada, com o mínimo de 20 (vinte) horas, em dias úteis, nas instalações da contratante, para no mínimo 5 (cinco) técnicos da PGE;

2.3.10 O treinamento ou hands-on deverá ser iniciado imediatamente após a instalação e configuração do parque computacional;

2.3.11 O treinamento ou hands-on deverá englobar, pelo menos, os seguintes aspectos:

2.3.11.1 Introdução ao software (conceitos, componentes e arquitetura);
2.3.11.2 Planejamento de uso (requisitos de ambiente para instalação);
2.3.11.3 Instalação e configuração do produto;
2.3.11.4 Aplicação de políticas de instalação automática, monitoramento e gerenciamento;
2.3.11.5 Técnicas de realização de backup e restore do banco de dados da aplicação;
2.3.11.6 Utilização de ferramentas de apoio, tais como, visualizador, relatórios, consultas, contingência do fabricante e procedimentos para instalação de patchs.

2.3.12 O Prazo de execução dos serviços de Instalação, Configuração e Treinamento para uso da solução de segurança no parque computacional da PGE deverá ser concluído em no máximo 30 (trinta) dias consecutivos, a contar da data da assinatura do Instrumento Contratual;

2.3.13 A empresa contratada deverá realizar duas avaliações durante o período de vigência do contrato, perante solicitação da contratante, do ambiente do PGE, mediante verificação de instalações e configurações de toda a solução de segurança, adequando-as às melhores práticas, essa atividade deve gerar relatório para posterior melhoria pela equipe da PGE;

2.3.14Todo suporte deve ser prestado por técnicos capacitados pelo fabricante;

2.3.15Caberá a PGE requisitar o suporte técnico, ficando a Contratada obrigada a realizá-lo, de acordo com o nível de severidade e nos prazos máximos.

2.3.16 O suporte técnico deverá ser prestado nas seguintes formas:

2.3.16.1 Plantão Telefônico, Website e E-mail - Serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;

2.3.16.2 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 previstos: suporte para *up-grade* de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; integração dos ambientes da configuração do software na rede da PGE. Neste caso a contratada deve possuir plantão de 08 (oito) horas por dia, 05 (cinco) dias por semana, para este tipo de atendimento;

2.3.16.3 O atendimento no local (on site) deve ser realizado na PGE, no seguinte endereço: 3ª Avenida Centro Administrativo da Bahia, 370 - CAB, Salvador - BA, 41745-005.

2.3.17 Para a execução do suporte técnico, a Contratada deverá contar com equipe técnica certificada pelo fabricante e com suporte ilimitado (quantidade de chamados) ao centro de suporte mundial do fabricante a nível internacional, a fim de garantir transferência diretamente ao fabricante dos problemas de maior complexidade que não tenham sido resolvidos em seu próprio laboratório;

2.3.18 O encaminhamento de chamados deverá ser efetuado pelos técnicos responsáveis no prazo máximo conforme os níveis de severidade indicados neste edital. Após este prazo, em caso de não solução, a Contratada deverá acionar o atendimento, no local designado pela PGE, de acordo com o nível de serviço acordado. O suporte prestado pela empresa terá chamados ilimitados;

2.3.19 A Contratada deverá responder aos acionamentos, dentro dos prazos fixados neste edital, a partir da abertura do acionamento;

2.3.20 O término do atendimento deverá ocorrer dentro dos prazos fixados no neste edital, a partir do contato do técnico da Contratada, responsável pelo atendimento;

2.3.21 Entende-se por início do atendimento a hora do contato do técnico de suporte da Contratada com a equipe da Contratante;

2.3.22 Entende-se por término de atendimento a disponibilidade do produto para uso em perfeitas condições de funcionamento no local onde está instalado;

2.3.23 O nível de severidade será informado pela PGE no momento da abertura de cada chamado;

2.3.24 O nível de severidade poderá ser reclassificado a critério da PGE. Caso isso ocorra haverá o início de nova contagem de prazo, conforme o novo nível de severidade;

2.3.25 Todas as solicitações de suporte técnico devem ser registradas pela empresa prestadora do serviço, para acompanhamento e controle da execução do serviço;

2.3.26 A Contratada deverá apresentar relatório de atendimento para cada solicitação de suporte, contendo data e hora da solicitação de suporte técnico, do início e do término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes;

2.3.27 O relatório de atendimento deverá ser assinado pelo servidor da PGE que solicitou o suporte técnico;

2.3.28 Para a execução do atendimento, é necessária a autorização da PGE para instalação ou desinstalação de qualquer software ou equipamentos que não façam parte da solução de segurança fornecida.

2.4. ACORDO NÍVEL DE SERVIÇO (ANS):

2.4.1 A Contratada deverá possuir Central de Atendimento (contato telefônico, sitio na Internet e e-mail) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 08 (oito) horas por dia, 05 (cinco) dias por semana;

2.4.2 A Contratada deverá prestar serviços de suporte técnico 08 horas por dia, 05 dias por semana, na cidade de Salvador (BA), relativos a prestação do serviço objeto deste Termo de Referência, sem ônus para a Contratante;

2.4.3 Para efeito dos atendimentos técnicos, a Contratada deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo;

2.4.4 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 ou em mídia digital) mediante solicitação.

2.4.5 A CONTRATADA deverá fazer análises dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe da CONTRATANTE.

2.4.6 A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.

2.4.7 A CONTRATADA deverá disponibilizar à CONTRATANTE serviço de atendimento de um Gestor do contrato de Suporte, responsável este que será o ponto focal de todas as necessidades de suporte da CONTRATANTE para casos de escalações ou problemas de atendimento do Suporte Técnico. Caso a CONTRATADA tenha seus laboratórios em outros países que não seja o território nacional, o Gestor deverá ter fluência na língua para facilitar a comunicação entre as partes.

2.4.8 A CONTRATANTE permitirá o acesso dos técnicos credenciados pela CONTRATADA às instalações onde se encontrarem os equipamentos com a solução de segurança instalada para a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança da CONTRATANTE, notadamente àquelas atinentes à identificação, trânsito e permanência nas dependências;

2.4.9 Mesmo se permitido pela CONTRATANTE, a permanência do técnico além do tempo de resolução do problema, para a continuidade de solução de um problema, não deverá representar qualquer ônus adicional à CONTRATANTE.

2.4.10 Níveis de Serviço e Tempo Esperados:

2.4.11 Plantão Telefônico por número 0800 como serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;

2.4.12 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 up-grade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; atualização simultânea nos ambientes dos órgãos e entidades da CONTRATANTE.

2.4.13 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, dúvidas gerais sobre a solução de segurança (software) fornecido.

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

2.4.14 Para o Nível 1, caso o atendimento não seja finalizado até as 20h00min, o técnico não poderá interrompê-lo, devendo continuar até sua finalização, ou a interrupção do mesmo pela Coordenação de Tecnologia e Gestão da Informação. Todo o chamado somente será caracterizado como "encerrado" mediante concordância da Coordenação de Tecnologia e Gestão da Informação;

2.4.15 Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, este deverá ser programado e planejado, com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da CONTRATANTE.

2.4.16 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 ofertada, sem ônus para a CONTRATANTE;

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

2.4.18 A CONTRATADA deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução, sem ônus para a CONTRATANTE durante 36 (trinta e seis) meses.

2.4.19 A licitante deverá ainda realizar os seguintes suportes proativos:

2.4.19.1Duas avaliações on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.

2.4.19.2 Uma avaliação on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução de gerência centralizada, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.

2.4.19.3 Quatro visitas técnicas on-site durante o ano de profissionais certificados pelo fabricante para apoiar nas implementações e nos controles gerados pelas ações proativas.

2.5 TESTE E VERIFICAÇÃO PRELIMINAR

2.5.1 Todos os componentes disponíveis no software fornecido serão testados por meio de procedimentos designados pela Contratante, findo os quais será elaborado relatório técnico com a análise dos resultados;

2.5.2 O processo de realização dos testes de verificação preliminar do software será desenvolvido de acordo com os eventos e atividades descritos a seguir:

2.5.2.1 Conferência da Entrega: consiste na identificação e conferência do software fornecido;

2.5.2.2 Teste de Instalação: consiste na verificação da instalação e da configuração das funcionalidades instaladas;

2.5.2.3 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;

2.5.2.4 Testes de Desempenho: consiste no acompanhamento do funcionamento do software implementado no âmbito da infraestrutura de rede da Contratante, em que serão aprofundados os testes funcionais e de otimização. Este período terá a duração de 15 (quinze) dias contados do término dos testes de ativação, podendo ser prorrogado por outro período de igual tamanho;

2.5.3 A verificação preliminar não implica em recebimento definitivo do software fornecido;

2.5.4 O relatório gerado em função dos Testes de Verificação Preliminar será documento integrante do Termo de Recebimento e Aceitação do software fornecido.

2.6 ENTREGA, ACEITE E INSTALAÇÃO:

2.6.1 O aceite do software será feito pela PGE, após a implantação e entrada em operação do software fornecido;

2.6.2 O aceite do software será feito mediante emissão pela "Comissão de Recebimento", nomeada pela PGE, do "Termo de Recebimento e Aceitação" dos Produtos;

2.6.3 A entrega e instalação do software será feita de acordo com plano de implantação, apresentado pela Contratada e aprovado pela Contratante;

2.6.4 A instalação deverá seguir cronograma previsto no plano de implantação;

2.6.5 Como parte dos documentos de aceite do software fornecido, a Contratada deverá apresentar "Tabela de Comprovação Técnica " das especificações exigidas neste Termo de Referência (apresentar na Tabela a correlação das especificações com a respectiva comprovação técnica, exemplo, página, item, documento, etc.). A comprovação técnica deverá ser efetuada através de documentos oficiais referentes ao produto fornecido, bem como referente aos módulos complementares.

2.7 DOCUMENTAÇÃO TÉCNICA:

2.7.1 A documentação técnica a ser fornecida deverá conter no mínimo os módulos descritos a seguir:

2.7.2 Documentação das Funcionalidades: Este documento conterá as características técnicas do produto e suas funções, procedimentos e parâmetros de configuração, tabelas, ilustrações, etc.;

2.7.3 Documentação de Instalação e Operação: Este documento conterá informações quanto aos procedimentos de instalação e operação, comandos e testes aplicáveis, procedimentos de inicialização, de configuração e gerência de desempenho, de falhas e de segurança pertinentes.

2.7.4 A Contratada deverá apresentar juntamente com a documentação dos produtos, certificado ou título, concedido pelo fabricante, que comprove o credenciamento da Contratada como representante autorizada para fornecimento de antivírus e antivírus para ambientes virtuais;

2.7.5 A Contratada deverá apresentar juntamente com a documentação do produto, as licenças dos produtos fornecidos necessários para a implantação;

2.7.6 A documentação dos produtos abrange: manuais operacionais dos produtos, documento com as especificações técnicas dos produtos e seus recursos, as licenças dos produtos, mídias contendo os produtos para instalação fornecidos e todas as documentações acessórias relativas aos produtos fornecidos.

3. Garantia Técnica:

(x) **3.1** O prazo legal de garantia técnica será de **30 (trinta) dias**, tratando-se de fornecimento de serviço e de produtos não duráveis, e de **90 (noventa) dias**, tratando-se de fornecimento de serviço e de produtos duráveis (art. 26, I e II do CDC).

3.1.1 Deverá ser acrescido ao prazo da garantia legal, a garantia (ou licenciamento) contratual de 36 (trinta e seis) meses.

3.1.2 A garantia contratual é complementar à legal e será conferida mediante termo escrito (art. 50 do CDC).

3.2 O termo de garantia ou equivalente deve ser padronizado e esclarecer, de maneira adequada, em que consiste, a forma, o prazo e o lugar em que pode ser exercitada, bem como os ônus a cargo do Contratante, devendo ser entregue devidamente preenchido, pela Contratada, no ato do fornecimento, acompanhada de manual de instrução e, quando for o caso, do manual de instalação e uso do produto, em linguagem didática, com ilustrações (art. 50, parágrafo único, do CDC).

ANEXO I DO TERMO DE REFERÊNCIA

ESPECIFICAÇÕES TÉCNICAS

Antivirus

LICENCA SOFTWARE ANTIVIRUS para estações de trabalho e servidores com console de gerenciamento.

- Microsoft Windows Server 2003 SP2 (Todas edições);
- Microsoft Windows Server 2003 x64 SP2 (Todas edições);
- Microsoft Windows Server 2008 (Todas edições);
- Microsoft Windows Server 2008 x64 SP1 (Todas edições);
- Microsoft Windows Server 2008 R2 (Todas edições);
- Microsoft Windows Server 2012 (Todas edições);

- Microsoft Windows Server 2012 R2 (Todas edições);
- Microsoft Windows Small Business Server 2003 SP2 (Todas edições);
- Microsoft Windows Small Business Server 2008 (Todas edições);
- Microsoft Windows Small Business Server 2011 (Todas edições);
- Microsoft Windows XP Professional SP2 ou superior;
- Microsoft Windows XP Professional x64 SP2 ou superior;
- Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;
- Microsoft Windows Vista Business / Enterprise / Ultimate SP1 x64 ou posterior;
- Microsoft Windows 7 Professional / Enterprise / Ultimate;
- Microsoft Windows 7 Professional / Enterprise / Ultimate x64;
- Microsoft Windows 8 Professional / Enterprise;
- Microsoft Windows 8 Professional / Enterprise x64;
- Microsoft Windows 8.1 Professional / Enterprise;
- Microsoft Windows 8.1 Professional / Enterprise x64.

Suporta as seguintes plataformas virtuais:

- VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5, ESXi 6.0;
- Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;
- KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS;
- Microsoft VirtualPC 6.0.156.0;
- Parallels Desktop 7 e superior;
- Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);
- Citrix XenServer 6.1, 6.2.

Características:

- A console deve ser acessada via WEB (HTTPS) ou MMC;
- Console deve ser baseada no modelo cliente/servidor;
- Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
- Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
- Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
- As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
- Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
- 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;
- Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
- A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
- Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
- Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema IOS, Android e Windows;
- Capacidade de instalar remotamente qualquer "app" em smartphones e tablets de sistema IOS;
- A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
- Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
- Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
- Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e IOS) protegidos pela solução de segurança;
- Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- 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;
- A comunicação entre o cliente e o servidor de administração deve ser criptografada;
- Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
- Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

  ✓ Nome do computador;

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

• Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
• Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
• Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
• 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;
• 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;
• 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;
• 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;
• Deve fornecer as seguintes informações dos computadores:

- ✓ Se o antivírus está instalado;
- ✓ Se o antivírus está iniciado;
- ✓ Se o antivírus está atualizado;
- ✓ Minutos/horas desde a última conexão da máquina com o servidor administrativo;
- ✓ Minutos/horas desde a última atualização de vacinas;
- ✓ Data e horário da última verificação executada na máquina;
- ✓ Versão do antivírus instalado na máquina;
- ✓ Se é necessário reiniciar o computador para aplicar mudanças;
- ✓ Data e horário de quando a máquina foi ligada;
- ✓ Quantidade de vírus encontrados (contador) na máquina;
- ✓ Nome do computador;
- ✓ Domínio ou grupo de trabalho do computador;
- ✓ Data e horário da última atualização de vacinas;
- ✓ Sistema operacional com Service Pack;
- ✓ Quantidade de processadores;
- ✓ Quantidade de memória RAM;
- ✓ Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
- ✓ Endereço IP;
- ✓ Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
- ✓ Atualizações do Windows Updates instaladas;
- ✓ Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
- ✓ Vulnerabilidades de aplicativos instalados na máquina;

• Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
• Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

- ✓ Alteração de Gateway Padrão;
- ✓ Alteração de subrede;
- ✓ Alteração de domínio;
- ✓ Alteração de servidor DHCP;
- ✓ Alteração de servidor DNS;
- ✓ Alteração de servidor WINS;
- ✓ Alteração de subrede;
- ✓ Resolução de Nome;
- ✓ Disponibilidade de endereço de conexão SSL;

• Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via Internet;
• Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
• Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

- Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 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;
- 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;
- Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
- Capacidade de gerar traps SNMP para monitoramento de eventos;
- Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
- Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
- Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
- 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;
- Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
- Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
- Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
  - ✓Nome do vírus;
  - ✓Nome do arquivo infectado;
  - ✓Data e hora da detecção;
  - ✓Nome da máquina ou endereço IP;
  - ✓Ação realizada.

- Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
- Capacidade de realizar inventário de hardware de todas as máquinas clientes;
- Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
- Capacidade de diferenciar máquinas virtuais de máquinas físicas.

Estações Windows

Compatibilidade:

- Microsoft Windows Embedded 8.0 Standard x64;
- Microsoft Windows Embedded 8.1 Industry Pro x64;
- Microsoft Windows Embedded Standard 7* x86 / x64 SP1;
- Microsoft Windows Embedded POSReady 7* x86 / x64;
- Microsoft Windows XP Professional x86 SP3 e superior;
- Microsoft Windows Vista x86 / x64SP2 e posterior;
- Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
- Microsoft Windows 8 Professional/Enterprise x86 / x64;
- Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
- Microsoft Windows 10 Pro / Enterprise x86 / x64.

Características:

Deve prover as seguintes proteções:

- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
- Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
- Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc);
- O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
- Firewall com IDS;
- Autoproteção (contra-ataques aos serviços/processos do antivírus);
- Controle de dispositivos externos;

- Controle de acesso a sites por categoria;
- Controle de acesso a sites por horário;
- Controle de acesso a sites por usuários;
- Controle de execução de aplicativos;
- Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 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;
- 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;
- Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- Capacidade de verificar somente arquivos novos e alterados;
- Capacidade de verificar objetos usando heurística;
- Capacidade de agendar uma pausa na verificação;
- Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
- Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

  ✓Perguntar o que fazer, ou bloquear acesso ao objeto;
  ✓Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
  ✓Caso positivo de desinfecção:Restaurar o objeto para uso;
  ✓Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

- Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 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);
- Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
- Capacidade de verificar links inseridos em e-mails contra phishings;
- Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
- Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

  ✓Perguntar o que fazer, ou;
  ✓Bloquear o e-mail;
  ✓Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
  ✓Caso positivo de desinfecção: restaurar o e-mail para o usuário;
  ✓Caso negativo de desinfecção:mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

- Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
- Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
- Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
- Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
- Deve ter suporte total ao protocolo IPv6;
- Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
- Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
- Perguntar o que fazer, ou;
- Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
- Permitir acesso ao objeto;
- O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

• Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
• Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;
• Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
• 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;
• Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
• 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;
• Deve possuir módulo de bloqueio de *Phishing*, com atualizações incluídas nas vacinas, obtidas pelo *Anti-Phishing Working Group* (http://www.antiphishing.org/);
• Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
• 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;
• O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

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

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

  ✓Discos de armazenamento locais;
  ✓Armazenamento removível;
  ✓Impressoras;
  ✓CD/DVD;
  ✓Drives de disquete;
  ✓Modems;
  ✓Dispositivos de fita;
  ✓Dispositivos multifuncionais;
  ✓Leitores de smart card;
  ✓Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
  ✓Wi-Fi;
  ✓Adaptadores de rede externos;
  ✓Dispositivos MP3 ou smartphones;
  ✓Dispositivos Bluetooth;
  ✓Câmeras e Scanners.

• Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
• Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
• Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
• Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
• 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;
• 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);
• Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
• 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;
• Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
• Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

Estações Mac OS X

Compatibilidade:

- Mac OS X 10.11 (El Capitan);
- Mac OS X 10.10 (Yosemite);
- Mac OS X 10.9 (Mavericks).
- Mac OS X 10.8 (Mountain Lion)
- Mac OS X 10.7 (Lion)

Características:

• Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
• Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
• 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;
• Deve possuir suportes a notificações utilizando o Growl;
• As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
• Capacidade de voltar para a base de dados de vacina anterior;
• Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
• 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;
• Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
• Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
• Capacidade de verificar somente arquivos novos e alterados;
• Capacidade de verificar objetos usando heurística;
• Capacidade de agendar uma pausa na verificação;
• O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

✓Perguntar o que fazer, ou;
✓Bloquear acesso ao objeto;
✓Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
✓Caso positivo de desinfecção:restaurar o objeto para uso;
✓Caso negativo de desinfecção: mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

• Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
• Capacidade de verificar arquivos de formato de email;
• 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;
• Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

Estações de trabalho Linux

Compatibilidade:

- **Plataforma 32-bits:**
  1. Canaima 3;
  2. Red Flag Desktop 6.0 SP2;
  3. Red Hat Enterprise Linux 5.8 Desktop;
  4. Red Hat Enterprise Linux 6.2 Desktop;
  5. Fedora 16;
  6. CentOS-6.2;
  7. SUSE Linux Enterprise Desktop 10 SP4;
  8. SUSE Linux Enterprise Desktop 11 SP2;
  9. openSUSE Linux 12.1;
  10. openSUSE Linux 12.2;
  11. Debian GNU/Linux 6.0.5;
  12. Mandriva Linux 2011;

13. Ubuntu 10.04 LTS;
14. Ubuntu 12.04 LTS.

- **Plataforma 64-bits:**
  1. Canaima 3;
  2. Red Flag Desktop 6.0 SP2;
  3. Red Hat Enterprise Linux 5.8;
  4. Red Hat Enterprise Linux 6.2 Desktop;
  5. Fedora 16;
  6. CentOS-6.2;
  7. SUSE Linux Enterprise Desktop 10 SP4;
  8. SUSE Linux Enterprise Desktop 11 SP2;
  9. openSUSE Linux 12.1;
  10. openSUSE Linux 12.2;
  11. Debian GNU/Linux 6.0.5;
  12. Ubuntu 10.04 LTS;
  13. Ubuntu 12.04 LTS.

Características:

- Deve prover as seguintes proteções:

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

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

✓Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
✓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;
✓Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
✓Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

- Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- Capacidade de verificar objetos usando heurística;
- Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

Servidores Windows

Compatibilidade:

- **Plataforma 32-bits:**

✓ Microsoft Windows Server 2003 Standard / Enterprise (SP2);
✓ Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);
✓ Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
✓ Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).

- **Plataforma 64-bits:**

✓Microsoft Windows Server 2003 Standard / Enterprise (SP2);

✓Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
✓Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
✓Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);

✓Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
✓Microsoft Windows Storage Server 2008 R2;
✓Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);
✓Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
✓Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
✓Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
✓Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
✓Microsoft Windows Storage Server 2012 (Todas edições);
✓Microsoft Windows Storage Server 2012 R2 (Todas edições);
✓Microsoft Windows Hyper-V Server 2012;
✓Microsoft Windows Hyper-V Server 2012 R2.

Características:

• Deve prover as seguintes proteções:

✓Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
✓ Auto-proteção contra-ataques aos serviços/processos do antivírus;
✓ Firewall com IDS;
✓ Controle de vulnerabilidades do Windows e dos aplicativos instalados;

• Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
• As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

✓ Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
✓ Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
✓ Leitura de configurações;
✓ Modificação de configurações;
✓ Gerenciamento de Backup e Quarentena;
✓ Visualização de relatórios;
✓ Gerenciamento de relatórios;
✓ Gerenciamento de chaves de licença;
✓ Gerenciamento de permissões (adicionar/excluir permissões acima);

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

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

• 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;
• Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
•Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (*uninterruptible Power supply – UPS*);
• Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;
• Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
• Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

- Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 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;
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- Capacidade de verificar somente arquivos novos e alterados;
- Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
- Capacidade de verificar objetos usando heurística;
- Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- Capacidade de agendar uma pausa na verificação;
- Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

  ✓Perguntar o que fazer, ou;
  ✓Bloquear acesso ao objeto;
  ✓Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
  ✓Caso positivo de desinfecção: restaurar o objeto para uso;
  ✓Caso negativo de desinfecção:mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

- Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

Servidores Linux

Compatibilidade:

Plataforma 32-bits:

- Red Hat Enterprise Linux Server 5.x;
- Red Hat® Enterprise Linux® Server 6.x (6.0 - 6.6);
- CentOS 6.x (6.0 - 6.6);
- SUSE® Linux Enterprise Server 11 SP3;
- Ubuntu Server 12.04 LTS;
- Ubuntu Server 14.04 LTS;
- Ubuntu Server 14.10;
- Oracle Linux 6.5;
- Debian GNU/Linux 7.5, 7.6, 7.7;
- openSUSE 13.1.
- Plataforma 64-bits:
- Red Hat Enterprise Linux Server 5.x;
- Red Hat Enterprise Linux Server 6.x (6.0 - 6.6);
- Red Hat Enterprise Linux Server 7;
- CentOS-6.x (6.0 - 6.6);
- CentOS-7.0;
- SUSE Linux Enterprise Server 11 SP3;
- SUSE Linux Enterprise Server 12;
- Novell Open Enterprise Server 11 SP1;
- Novell Open Enterprise Server 11 SP2;
- Ubuntu Server 12.04 LTS;
- Ubuntu Server 14.04 LTS;
- Ubuntu Server 14.10;
- Oracle Linux 6.5;
- Oracle Linux 7.0;
- Debian GNU/Linux 7.5, 7.6, 7.7;

- openSUSE® 13.1.

Características:

- Deve prover as seguintes proteções:

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

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

  ✓Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
  ✓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;
  ✓Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
  ✓Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

- Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- Capacidade de verificar objetos usando heurística;
- Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

Servidores Novell Netware:

Compatibilidade:

- ✓ Novell Netware 5.x Support Pack 6 ou superior;
- ✓ Novell Netware 6.0 Support Pack 3 ou superior;
- ✓ Novell Netware 6.5 Support Pack 3 ou superior.

Características:

- Deve possuir proteção em tempo real para arquivos acessados, criados ou modificados;
- Deve possuir verificação manual e agendada de acordo com a configuração do administrador;
- Capacidade de realizar update de maneira automatica, via Internet ou LAN;
- Capacidade de fazer um rollback das vacinas;
- Capacidade de mover arquivos suspeitos ou infectados para área de quarentena;
- Capacidade de criar logs detalhados e salvar resultados das verificações agendadas;
- Capacidade de salvar um backup de todos os objetos infectados e suspeitos tratados;
- Capacidade de notificar o administrador de varreduras concluídas e sobre objetos maliciosos encontrados no servidor, utilizando a rede Novell ou e-mail.

Smartphones e tablets

Compatibilidade:

- ✓ Apple IOS 7.0 – 8.X;
- ✓ Windows Phone 8.1;
- ✓ Android OS 2.3 – 5.1.

Características:

• Deve prover as seguintes proteções:

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

✓Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;
✓Arquivos abertos no smartphone;
✓Programas instalados usando a interface do smartphone

• Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
• Deverá isolar em área de quarentena os arquivos infectados;
• Deverá atualizar as bases de vacinas de modo agendado;
• Deverá bloquear spams de SMS através de Black lists;
• Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;
• Capacidade de desativar por política: Wi-fi; Câmera; Bluetooth.
• Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
• Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
• Deverá ter firewall pessoal (Android);

• Capacidade de tirar fotos quando a senha for inserida incorretamente;
• Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

• Capacidade de enviar comandos remotamente de:

✓Localizar;
✓Bloquear.

• Capacidade de detectar Jailbreak em dispositivos IOS;
• Capacidade de bloquear o acesso a site por categoria em dispositivos;
• Capacidade de bloquear o acesso a sites phishing ou malicioso;
• Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
• Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído;
• Capacidade de configurar White e blacklist de aplicativos;
• Capacidade de localizar o dispositivo quando necessário;
• Permitir atualização das definições quando estiver em "roaming";
• Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
• Capacidade de enviar URL de instalação por e-mail;
• Capacidade de fazer a instalação através de um link QRCode;

• Capacidade de executar as seguintes ações caso a desinfecção falhe:

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

Gerenciamento de dispositivos móveis (MDM)

Compatibilidade:

Dispositivos conectados através do Microsoft Exchange ActiveSync:

- ✓ Apple IOS;
- ✓ Windows Phone;
- ✓ Android.

Dispositivos com suporte ao Apple Push Notification (APNs).

- ✓ Apple IOS 3.0 ou superior.

Características:

- Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
- Capacidade de ajustar as configurações de:

  - ✓ Sincronização de e-mail;
  - ✓ Uso de aplicativos;
  - ✓ Senha do usuário;
  - ✓ Criptografia de dados;
  - ✓ Conexão de mídia removível.

- Capacidade de instalar certificados digitais em dispositivos móveis;
- Capacidade de, remotamente, resetar a senha de dispositivos IOS;
- Capacidade de, remotamente, apagar todos os dados de dispositivos IOS;
- Capacidade de, remotamente, bloquear um dispositivo IOS.

Criptografia

Compatibilidade:

Microsoft Windows XP Professional SP3 ou superior;
Microsoft Windows Vista Business/Enterprise/Ultimate SP2;
Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2;
Microsoft Windows 7 Professional/Enterprise/Ultimate;
Microsoft Windows 7 Professional/Enterprise/Ultimate x64;
Microsoft Windows 8 Professional/Enterprise;
Microsoft Windows 8 Professional/Enterprise x64;
Microsoft Windows 8.1 Professional / Enterprise;
Microsoft Windows 8.1 Professional / Enterprise x64;
Microsoft Windows 10 Pro x86 / x64;
Microsoft Windows 10 Enterprise x86 /x64.

Características:

- 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;
- Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
- Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
- Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;
- Permitir criar vários usuários de autenticação pré-boot;
- Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
- Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

  - ✓ Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
  - ✓ Criptografar todos os arquivos individualmente;
  - ✓ Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
  - ✓ Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

- 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;
- Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
- Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
- Verifica compatibilidade de hardware antes de aplicar a criptografia;
- Possibilita estabelecer parâmetros para a senha de criptografia;

- Bloqueia o reuso de senhas;
- Bloqueia a senha após um número de tentativas pré-estabelecidas;
- Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
- Permite criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo
- Permite criptografar as seguintes pastas pré-definidas: "meus documentos", "Favoritos", "Desktop", "Arquivos temporários" e "Arquivos do outlook";
- Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
- Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
- Permite criar um grupo de extensões de arquivos a serem criptografados;
- Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
- Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

Gerenciamento de Sistemas

- Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;
- Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
- 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;
- 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;
- Capacidade de gerenciar licenças de softwares de terceiros;
- Capacidade de registrar mudanças de hardware nas máquinas gerenciadas
- 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;
- Possibilita fazer distribuição de software de forma manual e agendada;
- Suporta modo de instalação silenciosa;
- Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
- Possibilita fazer a distribuição através de agentes de atualização;
- Utiliza tecnologia multicast para evitar tráfego na rede;
- Possibilita criar um inventário centralizado de imagens;
- Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
- Suporte a WakeOnLan para deploy de imagens;
- Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
- Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
- Capacidade de gerar relatórios de vulnerabilidades e patches;
- Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
- Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
- Permite baixar atualizações para o computador sem efetuar a instalação
- Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
- Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
- Permite selecionar produtos a serem atualizados pela console de gerenciamento;
- Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

ANEXO II

[illegible]

VTECH

DOS PREÇOS

[illegible]	ESPECIFICAÇÕES	[illegible]	[illegible]	[illegible]
01	[illegible] Fornecimento de licença de Software antivírus, Kaspersky Security for Business ADVANCED para estações de trabalho e servidores com console de gerenciamento, contendo serviço de instalação, configuração e suporte on-site. Com garantia de 36 (trinta e seis) meses. Marca/Modelo: Kaspersky Security for Business ADVANCED, Fabricante: Kaspersky, Procedência Russa.	1000	R$ 99,60	R$ 99.600,00

Valor Total da proposta R$ 99.600,00 (Noventa e nove mil e seiscentos reais).

O prazo de entrega será de até 30 (trinta) dias, contados da data da assinatura do contrato.

Prazo de licenciamento, período de garantia de 36 meses com atendimento ON-SITE em até 4 horas.

Transferência de conhecimento à equipe da PGE de toda solução ofertada com carga horária mínima de 20 horas.

Local de prestação de serviço: Os serviços serão prestados na Sede da Procuradoria Geral do Estado, situada na 3ª Avenida, 370, Centro Administrativo da Bahia, CEP: 41.745-005, Salvador/BA.

No preço total já estão incluídas todas e quaisquer despesas necessárias para o fiel cumprimento do objeto desta licitação, inclusive todos os custos com material de consumo, salários, encargos sociais, previdenciários e trabalhistas de todo o pessoal da VTECH, como também fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento desta proposta, bem como outras despesas decorrentes do cumprimento do objeto da proposta.

VTECH COMÉRCIO, SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA EIRELI
Avenida Santos Dumont, 5461, Km 5,5, Loja 155, Shopping Parque Norte, Estrada do Coco, Lauro de Freitas, Bahia, CEP 42.700-000

RAMOS LTDA, CNPJ 17.326.677/0001-17, que venceu lote único do pregão totalizando o valor de R$ 212,40 (duzentos e doze reais e quarenta centavos). Guanambi-Ba, 15/01/2019. Lucio Barreto do Nascimento - Cap PM, Pregoeiro Oficial.

RESULTADO ADJUDICAÇÃO E HOMOLOGAÇÃO DE LICITAÇÃO PREGÃO PRESENCIAL N.º 26/2018/SSP/ 17º BPM/GUANAMBI

O PREGOEIRO OFICIAL DO 17º BPM/GUANAMBI, em conformidade com a Lei Estadual nº 9.433/2005 e disposições do Edital da Licitação, torna público o resultado da licitação acima referenciada. Objeto: Fornecimento de lanches em kit. Empresa adjucatária: LOPES DINIZ EMPREENDIMENTOS LTDA, CNPJ 10.766.438/0001-39, que venceu lote único do pregão totalizando o valor de R$ 2.478,00 (dois mil, quatrocentos e setenta e oito reais). Guanambi-Ba, 15/01/2019. Lucio Barreto do Nascimento - Cap PM, Pregoeiro Oficial. **HOMOLOGAÇÃO:** O Major PM José Roberto Suarez Sant'anna, Respondendo pelo Comando do 17º BPM, no uso de suas atribuições delegadas através da Portaria Nº 19-CG/18, em conformidade com o art. 112, XVI, Lei Estadual nº 9.433/2005, homologa os resultados dos Pregões Presenciais nº 25 e 26/2018, para os objetos adjudicados supramencionados. Guanambi-BA, 17/01/2019.

RESULTADO DE LICITAÇÃO PREGÃO ELETRÔNICO N.º DAL 035/ 2018/SSPBA/PMBA/ DEPARTAMENTO DE APOIO LOGÍSTICO

A Pregoeira Oficial da PMBA/DAL, em conformidade com a Lei Estadual 9.433/05 e disposições do Edital da licitação, torna público o resultado da licitação acima referenciada. Objeto: Prestação do Serviço de conservação e limpeza para o DAL/PMBA. Empresa Adjudicatária: DLB Manutenção e Conservação Ltda-Me, CNPJ 12.262.420/0001-97. Lote único - Valor Total: R$ 195.797,72 (cento e noventa e seis mil setecentos e noventa e sete reais e setenta e dois centavos) - Daiane Regina da Hora Ferreira - Cap PM Pregoeira Oficial. **HOMOLOGAÇÃO**

O Comandante Geral, no uso de suas atribuições, em conformidade com o art. 112, Inciso XVI da Lei Estadual 9.433/05, homologa o resultado do Pregão Eletrônico Nº DAL 035/2018, para o objeto adjudicado supramencionado. Salvador, BA 17/01/2019. Anselmo Alves Brandão - Cel PM - Cmt Geral da PMBA.

CONTRATOS

PROCURADORIA GERAL DO ESTADO

RESUMO DE CONTRATO

Processo SEI nº 006.0409.2018.0001444-39
Contrato nº PGE 005/2019
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: **VTECH COMÉRCIO SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA**
Objeto: Serviço de licença de software antivirus para estações de trabalho e servidores em console de gerenciamento, contendo serviço de instalação, configuração e suporte on-site, no valor global estimado de R$ 99.600,00 (noventa e nove mil e seiscentos reais), Unidade Orçamentária - 06.601, Fonte - 154, Projeto/Atividade - 7033, Elemento de Despesa - 33.90.39 Prazo: 36 (trinta e seis) meses a partir da data da assinatura (17/01/2019).

RESUMO DE ADITIVO CONTRATUAL
Termo Aditivo 01 (Contrato PGE 011/2018)
Processo nº PGE/2018109648
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: **WEBTRIP AGÊNCIA DE VIAGENS E TURISMO LTDA - ME**
Objeto: Prorrogar o contrato por 12 (doze) meses, com início em 01/02/2019 e término em 31/01/2020, cujas despesas serão atendidas pela Unidade Orçamentária - 06.601, Fonte - 154, Projeto/Atividade - 1260, Elemento de Despesa - 33.90.33, retificadas as cláusulas em desacordo com as modificações ora inseridas e ratificadas as demais.

SECRETARIA DA ADMINISTRAÇÃO

RESUMO DO 4º TERMO ADITIVO AO CONTRATO Nº 038/2016
Processo SEI nº: 009.0231.2018.0016646-15. **Contratante:** Estado da Bahia, através da Secretaria da Administração. **Contratada**: Petrobrás Distribuidora S.A. **Objeto**: Prorrogar o prazo de vigência do contrato por 90 (noventa) dias, a contar de 30.01.2019. **Assinatura**: 16.01.2019.

Departamento Estadual de Trânsito – DETRAN

RESUMO DE CONTRATO

PROCESSO: 2018/106894-6 - **CONTRATO 002/2019 - PREGÃO ELETRÔNICO 015/2018 REGIME DE EXECUÇÃO:** SERVIÇOS COM EMPREITADA POR PREÇOS - **CONTRATANTE**: DEPARTAMENTO ESTADUAL DE TRÂNSITO - DETRAN/BA - **CONTRATADA**: CONSÓRCIO INETRNOVA - **OBJETO:** CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE IMPRESSÃO DE FORMULÁRIO, COMPREENDENDO EMISSÃO, ENVELOPAMENTO E A CAPTURA DE IMAGENS, PARA CARTEIRA NACIONAL DE HABILITAÇÃO - CNH E PERMISSÃO INTERNACIONAL PARA DIRIGIR - PID- **VIGÊNCIA: 17/01/2019 A 17/01/2020** - VALOR GLOBAL DE **R$ 32.497.920,00 (TRINTA E DOIS MILHÕES QUATROCENTOS E NOVENTA E SETE MIL NOVECENTOS E VINTE REAIS) - PAGAMENTO:** EM CONSONÂNCIA COM O §5º DO ART. 6º, COMBINADO COM A LETRA "A" DO INC. XI DO ART. 79 DA LEI 9.433/05, OS PAGAMENTOS DEVIDOS À CONTRATADA SERÃO EFETUADOS ATRAVÉS DE ORDEM BANCÁRIA OU CRÉDITO EM CONTA CORRENTE, NO PRAZO NÃO SUPERIOR A 08 (OITO) DIAS, CONTADOS DA DATA DE VERIFICAÇÃO DO ADIMPLEMENTO DE CADA PARCELA, O QUE DEVERÁ OCORRER NO PRAZO DE 15 (QUINZE) DIAS.. - **UNIDADE ORÇAMENTÁRIA/ GESTORA:** 09.301.0001 - **FUNÇÃO DE GOVERNO:** 06.122.218 - **ATIVIDADE:** 2922 9900 - **NATUREZA DA DESPESA:** 3390 3900 - **DESTINAÇÃO** : 0.105.000.000- **ASSINATURA** : 17/01/2019 - LUCIO GOMES BARROS PEREIRA - DIRETOR GERAL.

SECRETARIA DE DESENVOLVIMENTO ECONÔMICO

RESUMO DO SEGUNDO TERMO ADITIVO AO CONTRATO Nº 001/2017
PROCESSO SDE Nº. 015.1536.2019.0000069-80. **CONTRATANTE**: Estado da Bahia, através da Secretaria de Desenvolvimento Econômico. **CONTRATADO**: TELEFÔNICA BRASIL S/A. **OBJETO**: Prorrogação do prazo de vigência por mais 12 (doze) meses. **VIGÊNCIA**: A partir de 19/01/2019 com termino em 18/01/2020.

SECRETARIA DA EDUCAÇÃO

Universidade do Estado da Bahia – UNEB

RESUMO DO(S) CONTRATOS: Nº 001/2019 - **PROCESSO Nº** 074.7070.2018.0015146-30; **CONTRATANTE: UNEB; CONTRATADA:** Convic Conservação e Serviços Gerais EIRELI; **OBJETO:** Contratação emergencial de serviços terceirizados de conservação, limpeza, suporte administrativo e apoio operacional a prédios públicos; **DISPENSA**: nº 001/2019; **VIGÊNCIA:** 90 dias; **VALOR TOTAL**: R$ 2.227.811,10; **DOTAÇÃO ORÇAMENTÁRIA:** Projeto/Atividade: 2000; Fonte: 114; Elemento de Despesa: 3390.37; **DATA DA ASSINATURA:** 17/01/2019.

Universidade Estadual do Sudoeste da Bahia – UESB

Res. Termo Aditivo nº 04 ao Contrato n.º 039/2014 - UESB / MACEDO RIBEIRO CONSTRUÇÕES E ELETRIFICAÇÕES LTDA - ME. Objeto: prorrogação do prazo de vigência do Contrato por mais 12 (doze) meses, tendo como termo inicial o dia 24/11/2018 e termo final o dia 24/11/2019, conforme o constante no processo nº 998302. Permanecem inalterados os valores unitários dos serviços a serem prestados pela CONTRATADA. Assinatura em: 07/11/2018.
LUIZ OTÁVIO DE MAGALHÃES - REITOR

Res. Termo Aditivo nº 10 ao Contrato de Concessão de Uso n.º 018/2013 - UESB / CÉLIA MARINA DIAS DOS SANTOS. Objeto: prorrogação do prazo de vigência do Contrato por mais 89 (oitenta e nove) dias, tendo como termo inicial o dia 08/02/2019 e termo final o dia 07/05/2019, conforme o constante no processo nº 072.4160.2018.0007020-31 (SEI-BA). A CONCESSIONÁRIA, pela utilização do bem cedido, pagará o valor total de R$ 3.831,27 (três mil, oitocentos e trinta e um reais e vinte e sete centavos). Assinatura em: 04/01/2019.

Res. Termo Aditivo nº 04 ao Contrato n.º 016/2017 - UESB / PRIME SERVIÇOS E EMPREENDIMENTOS EIRELI EPP. Objeto: prorrogação do prazo de vigência do Contrato por mais 06 (seis) meses, tendo como termo inicial o dia 01/01/2019 e termo final o dia 01/07/2019, bem como a revisão da variação salarial , de 6% (seis por cento), concedida a partir de julho de 2018, através da Convenção Coletiva de Trabalho 2017/2018, celebrada entre o SEAC-BA (Sindicato das Empresas de Asseio e Conservação da Bahia) e o SINDILIMP-BA (Sindicato dos Trabalhadores em Limpeza Pública, Coml Indl, Hospitalar, Asseio, Prestação de Serviços em Geral, Conservação, Jardinagem e Controle de Pragas Intermunicipal, conforme o constante no processo nº 072.4160.2018.0006480-70 (SEI-BA). Valor global semestral de R$ 1.409.911,94 (um milhão, quatrocentos e nove mil, novecentos e onze reais e noventa e quatro centavos). Assinatura em: 28/12/2018.
LUIZ OTÁVIO DE MAGALHÃES- REITOR

Res. Termo Aditivo nº 03 ao Contrato n.º 032/2015 - UESB/ STERICYCLE GESTÃO AMBIENTAL LTDA. Objeto: prorrogação do prazo do Contrato firmado entre as partes, por mais 12 (doze) meses, tendo como termo inicial o dia 26/10/2018 e termo final o dia 26/10/2019, conforme o constante no processo nº 991371. Valor global estimado de R$ 65.700,00 (sessenta e cinco mil e setecentos reais). Assinatura em: 24/10/2018.
LUIZ OTÁVIO DE MAGALHÃES - REITOR

Universidade Estadual de Santa Cruz – UESC

RESUMO DE TERMOS ADITIVOS DE CONTRATOS - UESC
TERMO ADITIVO Nº 01 - CONTRATO Nº 1172017: TATTIANA CORTÊS FARIAS DE MENDONÇA; **PROC. SEI-BA Nº 073.6796.2018.0005146-75; Objeto;** Prorrogação do prazo de vigência do Contrato pelo prazo de 6(seis) meses, a contar de 13 de fevereiro de 2019. **Assinatura:** 16/01/2019.