GOVERNO DO ESTADO DA BAHIA
Procuradoria Geral do Estado
COORDENAÇÃO DE CONTRATOS - PGE/DG/DA/CC

Modalidade de Licitação	Número
Pregão Eletrônico	004/2022

CONTRATO QUE ENTRE SI CELEBRAM O ESTADO DA BAHIA, POR INTERMÉDIO DA PROCURADORIA GERAL DO ESTADO E A VTECH COMÉRCIO SERVICOS E EQUIPAMENTOS DE INFORMATICA PARA OS FINS QUE NELE SE DECLARAM.

CONTRATO Nº 015/2022

O **ESTADO DA BAHIA**, por intermédio da **PROCURADORIA GERAL DO ESTADO**, CNPJ nº. 04.139.403/0001-77, situada na 3ª Avenida, n°. 370, Centro Administrativo da Bahia, CEP 41.745-005, Salvador/BA, neste ato representada pelo seu titular **DR. PAULO MORENO CARVALHO**, autorizado pelo Decreto de delegação de competência publicado no D.O.E. de 08/01/2015, doravante denominado **CONTRATANTE**, e a **VTECH COMÉRCIO SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA**, CNPJ nº 22.122.370/0001-34, Inscrição Estadual nº 123.555.216, situada na Avenida Santos Dumont, 4487, Km 3,5, Loja 157, Shopping Passeo Norte, Estrada do Coco, Lauro de Freitas/BA, neste ato representada pela Sra. **NATASHA DE MATOS OLIVEIRA ARAÚJO**, portador da cédula de identidade nº 04.705.945-19, emitida por SSP/BA, inscrito no CPF/MF sob o nº 628.604.105-20, adjudicatária do pregão eletrônico nº 004/2022, processo administrativo nº 006.0409.2021.0039114-85 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 Renovação de licença/garantia das licenças de software antivírus utilizadas nas estações de trabalho e servidores da PGE, com garantia, contendo serviço de configuração/atualização e suporte *on site*, 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.

[SERVIÇOS NÃO-CONTÍNUOS]

CLÁUSULA SEGUNDA – PRAZO

O prazo de vigência do contrato, a contar da data (**x**) da sua assinatura, será de 36 (trinta e seis) meses.

§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:

[SERVIÇOS]

LOTE ÚNICO					
ITEM	**Descrição - Código SIMPAS**	**Unidade de Fornecimento (UF)**	**Quantitativo**	**PREÇO UNITÁRIO**	**PREÇO MENSAL**
1	RENOVAÇÃO DE LICENÇA DE USO DE SOFTWARE, Kaspersky Endpoint Security for Business advanced, com suporte e atualização. Para estações de trabalho e servidores pelo período de 36 (trinta e seis) meses Código SIMPAS: 02.81.23.00000301-8	**UN**	**1.000**	R$ 162,94	R$ 162.940,00
VALOR ESTIMADO GLOBAL					**R$ 162.940,00**

§1º Estima-se para o contrato o valor global de R$ 162.940,00 (cento e sessenta e dois mil novecentos e quarenta 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, tributos, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela CONTRATADA das obrigações.

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
06.601	03	126	218	7033
Região/planejamento	Natureza da despesa	Destinação do recurso	Tipo de recurso orçamentário	
7800	339040	154	Normal	

CLÁUSULA SÉTIMA – OBRIGAÇÕES DA CONTRATADA

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

[SERVIÇOS EM GERAL]

I. designar de sua estrutura administrativa um preposto permanentemente responsável pela perfeita execução do contrato, inclusive para atendimento de emergência, servindo de interlocutor e canal de comunicação entre as partes;

II. executar o 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 do 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;

XVII. prover as instalações, aparelhamento e pessoal técnico exigidos na licitação;

XVIII. alocar durante todo o período de execução do objeto a equipe técnica mínima exigida no instrumento convocatório, admitindo-se a sua substituição por profissionais de experiência equivalente ou superior, desde que aprovada pelo CONTRATANTE.

XIX. providenciar o cadastramento de seu representante legal ou procurador no site www.comprasnet.ba.gov.br, para a prática de atos através do Sistema Eletrônico de Informações – SEI.

Parágrafo único. Além das determinações acima descritas, a CONTRATADA que estiver sujeita à 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, deverá, no que concerne à aprendizagem:

a) recrutar, preferencialmente, para a contratação de aprendizes prevista no 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;

b) 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.

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

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 nº 9.433/05.

§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 Compete especificamente à fiscalização, sem prejuízo de outras obrigações legais ou contratuais:

I. exigir da CONTRATADA o cumprimento integral das obrigações pactuadas;

II. rejeitar todo e qualquer material de má qualidade ou não especificado;

III. relatar ao Gestor do Contrato ocorrências ou circunstâncias que possam acarretar dificuldades no desenvolvimento dos serviços em relação a terceiros;

IV. dar à autoridade superior imediata ciência de fatos que possam levar à aplicação de penalidades contra a CONTRATADA, ou mesmo à rescisão do contrato.

§4º Fica indicada como a área responsável pela gestão do contrato: Coordenação de Gestão Estratégica - CGE.

§5º Fica indicado como gestor deste Contrato o servidor: Eduardo Jorge Rodrigues Brandão, matrícula: 06.577.805-8.

§6º Fica indicado como fiscal deste Contrato o servidor: Mauricio de Cerqueira Pereira, matrícula: 06.579.186-0.

CLÁUSULA DÉCIMA – RECEBIMENTO DO OBJETO

O recebimento do objeto, consistente na aferição da efetiva prestação do serviço, realização da obra, entrega do bem ou de parcela destes, 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.

§1º Nos casos de aquisição de equipamentos de grande vulto, o recebimento definitivo far-se-á mediante termo circunstanciado e, nos demais,

mediante recibo.

§2º Na hipótese de não ser lavrado o termo circunstanciado ou de não ser procedida a verificação dentro dos prazos fixados, reputar-se-ão como realizados, desde que comunicados ao CONTRATANTE nos 15 (quinze) dias anteriores à exaustão dos mesmos

§3º O recebimento definitivo de 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.

§4º Esgotado o prazo de vencimento do recebimento provisório sem qualquer manifestação do CONTRATANTE, não dispondo o TERMO DE REFERÊNCIA de forma diversa, considerar-se-á definitivamente aceito pela Administração o objeto contratual, para todos os efeitos.

§5º Poderá ser dispensado o recebimento provisório nos seguintes casos:

I. gêneros perecíveis e alimentação preparada;

II. serviços profissionais;

III. serviços de valor até o limite previsto para compras e serviços, que não sejam de engenharia, na modalidade de convite, desde que não se componham de aparelhos, equipamentos e instalações sujeitos à verificação de funcionamento e produtividade.

§6º Salvo disposições em contrário constantes do TERMO DE REFERÊNCIA, os ensaios, testes e demais provas exigidas por normas técnicas oficiais para a boa execução do objeto do contrato correm por conta do contratado.

§7º O CONTRATANTE rejeitará, no todo ou em parte, obra, serviço ou fornecimento em desacordo com as condições pactuadas, podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis.

§8º 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.

§9º Com a conclusão da etapa do recebimento definitivo, a CONTRATADA estará habilitada a apresentar as nota(s) fiscal(is)/fatura(s) para pagamento.

CLÁUSULA DÉCIMA–PRIMEIRA - PAGAMENTO

Os pagamentos devidos à CONTRATADA serão efetuados através de ordem bancária ou crédito em conta aberta em instituição financeira contratada pelo Estado da Bahia, 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 As notas fiscais/faturas somente deverão ser apresentadas 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 As notas fiscais/faturas deverão atender as exigências legais pertinentes aos tributos e encargos relacionados com a obrigação, sujeitando-se às retenções tributárias previstas em lei, e, as situações específicas, à adoção da forma eletrônica.

§5º O processo de pagamento, para efeito do art. 126, inciso XVI, da Lei estadual nº 9.433/05, deverá ser instruído com a prova da manutenção d qualificação exigidas no certame, o que poderá ser aferido mediante consulta ao Registro Cadastral ou a sites oficiais, considerando demonstração a data de conclusão da etapa do recebimento definitivo.

§6º Em havendo alguma pendência impeditiva do pagamento, a exemplo de erro na apresentação da nota fiscal/fatura ou dos documentos pertine de circunstância que impeça a liquidação da despesa, como obrigações financeiras pendentes, decorrentes de penalidade imposta ou inadi sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a com situação, não acarretando qualquer ônus para o CONTRATANTE.

§7º Em caso de mora nos pagamentos devidos pelo CONTRATANTE, será observado o que se segue:

I. a atualização monetária será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a v *rata tempore*;

II. nas compras para entrega imediata, assim entendidas aquelas com prazo de entrega até 15 (quinze) dias contados da data da celebração atualização financeira correspondente ao período compreendido entre as datas do adimplemento e a prevista para o pagamento, desde qu em conformidade com o inc. II do art. 82 da Lei nº 9.433/05.

§8º Optando a CONTRATADA por receber os créditos em instituição financeira diversa da indicada no **caput**, deverá arcar com os custos de trans serão deduzidos dos pagamentos devidos.

CLÁUSULA DÉCIMA-SEGUNDA – 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-TERCEIRA– 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.

CLÁUSULA DÉCIMA-QUARTA 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 da CONTRATADA, será este ressarcido dos prejuízos regularmente comprovados que houver sofrido, na forma do §2º do art. 168 do mesmo diploma.

CLÁUSULA DÉCIMA-QUINTA – 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-SEXTA – 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 res 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 de 10% (dez por cento) incidente sobre o val

II. Caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicado o percentual de 10% (dez por cento) so 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, a de 0,7% (sete décimos por cento) por cada dia subseqüente ao trigésimo, calculados sobre o valor da parcela do fornecimento ou do serv

§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 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.

IV. Caso não seja possível identificar o valor ou custo da obrigação acessória descumprida, a multa será arbitrada pelo CONTRANTE, em valor que não supere 1% da sanção pecuniária que seria cabível pelo descumprimento da obrigação principal.

§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-SÉTIMA VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO

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

CLÁUSULA DÉCIMA-OITAVA COMUNICAÇÃO ELETRÔNICA

Fica pactuado que os atos de comunicação processual com a CONTRATADA poderão ser realizados por meio eletrônico, na forma do disposto na Lei nº 12.290, de 20 de abril de 2011, e do Decreto nº 15.805, de 30 de dezembro de 2014.

Parágrafo único. A CONTRATADA deverá manter atualizado o endereço eletrônico cadastrado no Sistema Eletrônico de Informações - SEI, para efeito do recebimento de notificação e intimação de atos processuais.

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, ____ de _____ de 20__.

CONTRATANTE	**CONTRATADA**
Testemunha	**Testemunha**

ANEXO I

SEÇÃO II TERMO DE REFERÊNCIA DO OBJETO DA LICITAÇÃO

1. DESCRITIVO: A presente licitação tem por objeto os itens abaixo descritos, conforme características, quantitativos, condições e especificações disciplinadas nesta

2. CARACTERÍSTICAS, QUANTITATIVOS, CRONOGRAMA/PRAZO DE ENTREGA E LOCAL DE ENTREGA:

LOTE ÚNICO

ITEM	Descrição	Unidade de Fornecimento (UF)	Quantitativo	Cronograma/Prazo
1	RENOVAÇÃO DE LICENÇA DE USO DE SOFTWARE, *Kaspersky Endpoint Security for Business advanced*, com suporte e atualização. Para estações de trabalho e servidores pelo período de 36 (trinta e seis) meses Código SIMPAS: 02.81.23.00000301-8	**UN**	**1.000**	Prazo de entrega: até 30 (trinta) dias, contados a partir da assinatura do contrato ou instr Período do licenciamento: 36 (trinta e seis) meses

2.1 LOCAL DA PRESTAÇÃO DE SERVIÇO

2.1.1 Os serviços serão prestados na sede da Procuradoria Geral do Estado, situada na 3ª Av. Centro Administrativo da Bahia, 370, CAB, Salvador – BA, CEP: 41.745-005 - Salvador – Bahia.

2.2 PERÍODO DE GARANTIA (OU DE LICENCIAMENTO)

2.2.1 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 deve 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.

2.2.2 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;

2.2.3 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;

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

3. ESPECIFICAÇÕES

3.1 GARANTIA TÉCNICA:

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

3.1.1 Deverá ser acrescido ao prazo da garantia legal, a garantia contratual de 36 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 exerc cargo do Contratante, devendo ser entregue devidamente preenchido, pela Contratada, no ato do fornecimento, acompanhada de manual de instrução e, quando for instalação e uso do produto, em linguagem didática, com ilustrações (art. 50, parágrafo único, do CDC).

3.3 CONDIÇÕES DE ENTREGA:

3.3.1 ENTREGA, ACEITE E INSTALAÇÃO

3.3.1.1 O aceite do software será feito pela PGE, após a implantação e entrada em operação do software fornecido;
3.3.1.2. O aceite do software será feito mediante emissão pela "Comissão de Recebimento", nomeada pela PGE, do "Termo de Recebimento e Aceitação" dos Produt
3.3.1.3. A entrega e instalação do software será feita de acordo com plano de implantação, apresentado pela Contratada e aprovado pela Contratante;
3.3.1.4. A instalação deverá seguir cronograma previsto no plano de implantação;
3.3.1.5. Como parte dos documentos de aceite do software fornecido, a Contratada deverá apresentar "Tabela de Comprovação Técnica " das especificações exigidas (apresentar na Tabela a correlação das especificações com a respectiva comprovação técnica, exemplo, página, item, documento, etc.). A comprovação técnica deverá s documentos oficiais referentes ao produto fornecido, bem como referente aos módulos complementares.

3.3.1.6. A Contratada deverá entregar os objetos contratados, acompanhados das respectiva Nota Fiscal no local indicado, onde será emitido o "Termo de Reconhecir Contratada. Depois de realizada a análise e estando o produto em conformidade com o previsto no edital, o setor requisitante através da "Comissão de Recebimento", i Recebimento Definitivo" do bem.

3.4 DISPOSIÇÕES ADICIONAIS:

3.4.1 SUPORTE TÉCNICO E ACORDO DE NÍVEL DE SERVIÇO

OBJETIVO:

Atender às necessidades da PGE para suporte técnico do antivírus, com o objetivo de proteger a rede corporativa e aumentar o nível de conformidade com a políti

3.4.1.1 EQUIPE TÉCNICA

Deve ser composta de técnicos capacitados pelo fabricante do software fornecido, e preparada para dar todo o suporte técnico e ajuda necessária para maximizar o software, aumentando a sua performance.

3.4.1.2 SUPORTE TÉCNICO

3.4.1.2.1 O suporte técnico ao produto fornecido deverá ser prestado através de contato Telefônico (telefone 0800 do fabricante ou telefone com numeração con Internet (website do fabricante ou do fornecedor), Correio Eletrônico (e-mail do fabricante ou do fornecedor) ou no Local (provido pelo fabricante ou pelo fornece emergência;
3.4.1.2.2. O suporte técnico deverá ser fornecido prioritariamente pelo fornecedor da solução de segurança ou pelo fabricante, no Brasil e na língua portuguesa;
3.4.1.2.3. Deverão ser executados pela empresa contratada serviços de Consultoria, Instalação e Configuração para uso da solução contratada com supervisão da
3.4.1.2.4. Deverá ser executada pela empresa contratada uma análise da situação atual e elaborar, em conjunto com a equipe interna da PGE, um plano de otimiz procedimentos e processos para o novo ambiente de segurança. Essa documentação deverá ser entregue, pela empresa contratada, em formato digital;
3.4.1.2.5. A empresa contratada deverá preservar todo ambiente computacional existente, de forma a manter a integridade dos dados, aplicativos e sistemas opera
3.4.1.2.6. A empresa contratada deverá preparar o ambiente de modo a operar conforme o estabelecido no plano de otimização de recursos, rotinas, procediment
3.4.1.2.7. 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 1 combinados entre o PGE e a contratada;
3.4.1.2.8. A instalação e configuração dos softwares adquiridos deverão ser executadas em 100% do Parque PGE, localizado em Salvador (BA);
3.4.1.2.9. O Prazo de execução dos serviços de Instalação, Configuração e para uso da solução de segurança no parque computacional da PGE deverá ser conclu consecutivos, a contar da data da assinatura do Instrumento Contratual;
3.4.1.2.10. A empresa contratada deverá realizar duas avaliações durante o período de vigência do contrato, perante solicitação da contratante, do ambiente do P instalações e configurações de toda a solução de segurança, adequando-as às melhores práticas, essa atividade deve gerar relatório para posterior melhoria pela equ
3.4.1.2.11. Todo suporte deve ser prestado por técnicos capacitados pelo fabricante;

3.4.1.2.12 Caberá a PGE requisitar o suporte técnico, ficando a Contratada obrigada a realizá-lo, de acordo com o nível de severidade e nos prazos máximos.
3.4.1.2.13. O suporte técnico deverá ser prestado nas seguintes formas:
3.4.1.2.14. Plantão Telefônico, Website e E-mail - Serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;
3.4.1.2.15. No Local (on site) - Serviço de uso ilimitado, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tip previstos: suporte para up-grade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à se software e do ambiente; integração dos ambientes da configuração do software na rede da PGE. Neste caso a contratada deve possuir plantão de 8 (oito) horas por para este tipo de atendimento;
3.4.1.2.16. Para a execução do suporte técnico, a Contratada deverá contar com equipe técnica certificada pelo fabricante e com suporte ilimitado (quantidade de mundial do fabricante a nível internacional, a fim de garantir transferência diretamente ao fabricante dos problemas de maior complexidade que não tenham sido r laboratório;
3.4.1.2.17. O encaminhamento de chamados deverá ser efetuado pelos técnicos responsáveis no prazo máximo conforme os níveis de severidade indicados neste 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 emp
3.4.1.2.18. O atendimento No Local (on site) deve ser provido na PGE, no seguinte endereço: 2ª Avenida Centro Administrativo da Bahia, 250 - CAB, Salvador
3.4.1.2.19. A Contratada deverá responder aos acionamentos, dentro dos prazos fixados neste edital, a partir da abertura do acionamento;
3.4.1.2.20. O término do atendimento deverá ocorrer dentro dos prazos fixados no neste edital, a partir do contato do técnico da Contratada, responsável pelo ate

3.4.1.2.21. Entende-se por início do atendimento a hora do contato do técnico de suporte da Contratada com a equipe da Contratante;
3.4.1.2.22. Entende-se por término de atendimento a disponibilidade do produto para uso em perfeitas condições de funcionamento no local onde está instalado;
3.4.1.2.23. O nível de severidade será informado pela Contratante no momento da abertura de cada chamado;
3.4.1.2.24. O nível de severidade poderá ser reclassificado a critério da Contratante. Caso isso ocorra haverá o início de nova contagem de prazo, conforme o no
3.4.1.2.25. Todas as solicitações de suporte técnico devem ser registradas pela Contratada, para acompanhamento e controle da execução do serviço;
3.4.1.2.26. A Contratada deverá apresentar relatório de atendimento para cada solicitação de suporte, contendo data e hora da solicitação de suporte técnico, do i atendimento, identificação do problema, providências adotadas e demais informações pertinentes;
3.4.1.2.27. O relatório de atendimento deverá ser assinado pelo servidor da Contratante que solicitou o suporte técnico;
3.4.1.2.28. Para a execução do atendimento, é necessária a autorização da Contratante para instalação ou desinstalação de qualquer software ou equipamentos qu segurança fornecida.

3.4.1.3 ACORDO DE NÍVEL DE SERVIÇO (ANS):

3.4.1.3.1 A Contratada deverá possuir Central de Atendimento (contato telefônico, sitio na Internet e e-mail) para consultas, aberturas de chamados técnicos e en durante 8 (oito) horas por dia, 5 (cinco) dias por semana;
3.4.1.3.2. A Contratada deverá prestar serviços de suporte técnico 8 horas por dia, 5 dias por semana, na cidade de Salvador (BA), relativos a prestação do serviç Referência, sem ônus para a Contratante;
3.4.1.3.3. Para efeito dos atendimentos técnicos, a Contratada deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo;
Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentad como outras geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à CONTRATANTE através de relatórios (impres mediante solicitação.

3.4.1.3.4. A CONTRATADA deverá fazer análises dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe d
3.4.1.3.5. A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.
3.4.1.3.6. A CONTRATADA deverá disponibilizar à CONTRATANTE serviço de atendimento de um Gestor do contrato de Suporte, responsável este que será o necessidades de suporte da CONTRATANTE para casos de escalações ou problemas de atendimento do Suporte Técnico. Caso a CONTRATADA tenha seus labo seja o território nacional, o Gestor deverá ter fluência na língua para facilitar a comunicação entre as partes.

3.4.1.3.7 A CONTRATANTE permitirá o acesso dos técnicos credenciados pela CONTRATADA às instalações onde se encontrarem os equipamentos com a sol a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança da CONTRATANTE, notadamente àquelas atin permanência nas dependências;
3.4.1.3.8. Mesmo se permitido pela CONTRATANTE, a permanência do técnico além do tempo de resolução do problema, para a continuidade de solução de un representar qualquer ônus adicional à CONTRATANTE.
3.4.1.3.9. Níveis de Serviço e Tempo Esperados:
3.4.1.3.10. Plantão Telefônico por número 0800 como serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;
3.4.1.3.11. No Local (on site) – Serviço de uso ilimitado, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes ti para up-grade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à perfo ambiente; atualização simultânea nos ambientes dos órgãos e entidades da CONTRATANTE.

3.4.1.3.12. 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 se

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
On Site	Término atendimento	2 horas	4 horas	72 horas
Telefone, e-mail e web	Início atendimento	-	-	24 horas
	Término atendimento	-	-	72 horas

3.4.1.3.13. - Para o Nível 1, caso o atendimento não seja finalizado até as 20h00min, o técnico não poderá interrompê-lo, devendo continuar até sua finalização, Coordenação de Tecnologia e Gestão da Informação. Todo o chamado somente será caracterizado como “encerrado” mediante concordância da Coordenação de T Informação;
3.4.1.3.14. - Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, este dev com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da CONTRATANTE.
3.4.1.3.15. A CONTRATADA deverá disponibilizar à CONTRATANTE um serviço preventivo de verificação e atualização de versões ou correções (patches) q específicos para a solução ofertada, sem ônus para a CONTRATANTE;
3.4.1.3.16. No caso de necessidade de ações preventivas ou corretivas a CONTRATANTE agendará com antecedência junto a CONTRATADA as implementaçõ comercial, preferencialmente em feriados e finais de semana, sem ônus para a CONTRATANTE;
3.4.1.3.17. A CONTRATADA deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da CONTRATANTE durante 36 (trinta e seis) meses.

3.4.1.3.18. A licitante deverá ainda realizar os seguintes suportes proativos:

3.4.1.3.18.1. Duas avaliações on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução, adequan segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.
3.4.1.3.18.2. Uma avaliação on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução de gerênci melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.
3.4.1.3.18.3. Quatro visitas técnicas on-site durante o ano de profissionais certificados pelo fabricante para apoiar nas implementações e nos controles gerados p

3.4.1.4. DOCUMENTAÇÃO TÉCNICA

3.4.1.4.1. A documentação técnica a ser fornecida deverá conter no mínimo os módulos descritos a seguir:
3.4.1.4.2. Documentação das Funcionalidades: Este documento conterá as características técnicas do produto e suas funções, procedimentos e parâmetros de con etc.;
3.4.1.4.3. Documentação de Instalação e Operação: Este documento conterá informações quanto aos procedimentos de instalação e operação, comandos e teste a inicialização, de configuração e gerência de desempenho, de falhas e de segurança pertinentes.
3.4.1.4.4. A Contratada deverá apresentar juntamente com a documentação dos produtos, certificado ou título, concedido pelo fabricante, que comprove o creden representante autorizada para fornecimento de antivírus e antivírus para ambientes virtuais;
3.4.1.4.5. A Contratada deverá apresentar juntamente com a documentação do produto, as licenças dos produtos fornecidos necessários para a implantação;
3.4.1.4.6. A documentação dos produtos abrange: manuais operacionais dos produtos, documento com as especificações técnicas dos produtos e seus recursos, a contendo os produtos para instalação fornecidos e toda documentação acessórias relativas aos produtos fornecidos.

3.4.1.5 TESTE E VERIFICAÇÃO PRELIMINAR

3.4.1.5.1 Todos os componentes disponíveis no software fornecido serão testados por meio de procedimentos designados pela Contratante, findo os quais será el análise dos resultados;
3.4.1.5.2. O processo de realização dos testes de verificação preliminar do software será desenvolvido de acordo com os eventos e atividades descritos a seguir:
3.4.1.5.3. Conferência da Entrega: consiste na identificação e conferência do software fornecido;
3.4.1.5.4. Teste de Instalação: consiste na verificação da instalação e da configuração das funcionalidades instaladas;

3.4.1.5.5. Testes de Ativação: consiste na operacionalização do software, após a conclusão dos testes de instalação, com a verificação de suas características, de compatibilidade;
3.4.1.5.6. Testes de Desempenho: consiste no acompanhamento do funcionamento do software implementado no âmbito da infraestrutura de rede da Contratante 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 pe
3.4.1.5.7. A verificação preliminar não implica em recebimento definitivo do software fornecido;
3.4.1.5.8. O relatório gerado em função dos Testes de Verificação Preliminar será documento integrante do Termo de Recebimento e Aceitação do software forn

3.4.1.6. UTILIZAÇÃO DE SOFTWARES

3.4.1.6.1. A CONTRATADA fornecerá, por sua conta, a instalação, configuração e licenças de todos os softwares que se fizerem necessários para a execução co decorrentes deste Termo de Referência.
3.4.1.6.2. Qualquer instalação de software em ambiente da CONTRATADA será precedida de justificativa, e somente será autorizado se for compatível com as e de seu provedor. Necessidades outras, além das descritas acima, serão arcadas pela própria CONTRATADA, as quais não serão passíveis de cobranças adicionais.

3.4.1.7. PROPRIEDADE INTELECTUAL

3.4.1.7.1. A Contratada entregará a Contratante toda e qualquer documentação gerada em função da prestação de serviços decorrente deste Termo de Referência. direitos patrimoniais autorais relativos aos resultados produzidos durante a vigência do Contrato são de propriedade exclusiva da Contratante, devidamente ampara Diretos Autorais, respeitados os direitos morais do autor. Entendem-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, desenhos, diagramas, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica. A Contratada fica proibida de veicular e comerciali informações geradas ou conhecidas relativas ao objeto da prestação dos serviços, salvo se houver a prévia autorização por escrito da Contratante

ANEXO I – DO TERMO DE REFERÊNCIA

ESPECIFICAÇÕES TÉCNICAS

1. Servidor de Administração e Console Administrativa

1.1. Compatibilidade:
1.1.1. Microsoft Windows Server 2012 Standard / Core / Foundation / Essentials / Datacenter x64;
1.1.2. Microsoft Storage Server 2012 e 2012 R2 x64;
1.1.3. Microsoft Windows Server 2012 R2 Standard / Core / Foundation / Essentials / Datacenter x64;
1.1.4. Microsoft Windows Server 2016 Standard / Core / Datacenter x64;
1.1.5. Microsoft Windows Server 2019 Standard / Core / Datacenter x64;
1.1.6. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
1.1.7. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
1.1.8. Microsoft Windows 8 Professional / Enterprise x64;
1.1.9. Microsoft Windows 8.1 Professional / Enterprise x32;
1.1.10. Microsoft Windows 8.1 Professional / Enterprise x64;
1.1.11. Microsoft Windows 10 x32;
1.1.12. Microsoft Windows 10 x64;

1.2. Suporta as seguintes plataformas virtuais:

1.2.1. Vmware: Workstation 15.x Pro, vSphere 6.5, vSphere 6.7;
1.2.2. Microsoft Hyper-V 2019;
1.2.5. Parallels Desktop 14;
1.2.7. Citrix XenServer 7.1;

1.3. Características:

1.3.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
1.3.2. Console deve ser baseada no modelo cliente/servidor;
1.3.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
1.3.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
1.3.5. Deve permitir incluir usuários do AD para logarem na console de administração
1.3.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptogra
1.3.7. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosc momento da expiração da licença;
1.3.8. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servid
1.3.9. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e
1.3.10. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
1.3.11. Deve armazenar histórico das alterações feitas em políticas;
1.3.12. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando alterada;
1.3.13. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
1.3.14. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
1.3.15. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
1.3.16. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;
1.3.17. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
1.3.18. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
1.3.19. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
1.3.20. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
1.3.21. Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;
1.3.22. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
1.3.23. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
1.3.24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

1.3.25. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenc
instalado nas máquinas clientes;
1.3.26. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
1.3.27. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
1.3.28. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâr
- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema Operacional;
- Máquina virtual.

1.3.29. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
1.3.30. 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 c
1.3.31. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
1.3.32. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas
proteção;
1.3.33. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estru
verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
1.3.34. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivíru
máquinas que não receberam atualização nos últimos 2 dias, etc;
1.3.35. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de
subgrupos;
1.3.36. Deve fornecer as seguintes informações dos computadores:
1.3.36.1. Se o antivírus está instalado;
1.3.36.2. Se o antivírus está iniciado;
1.3.36.3. Se o antivírus está atualizado;
1.3.36.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
1.3.36.5. Minutos/horas desde a última atualização de vacinas;
1.3.36.6. Data e horário da última verificação executada na máquina;
1.3.36.7. Versão do antivírus instalado na máquina;
1.3.36.8. Se é necessário reiniciar o computador para aplicar mudanças;
1.3.36.9. Data e horário de quando a máquina foi ligada;
1.3.36.10. Quantidade de vírus encontrados (contador) na máquina;
1.3.36.11. Nome do computador;
1.3.36.12. Domínio ou grupo de trabalho do computador;
1.3.36.13. Data e horário da última atualização de vacinas;
1.3.36.14. Sistema operacional com Service Pack;
1.3.36.15. Quantidade de processadores;
1.3.36.16. Quantidade de memória RAM;
1.3.36.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
1.3.36.18. Endereço IP;
1.3.36.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
1.3.36.20. Atualizações do Windows Updates instaladas;
1.3.36.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptad
CD/DVD;
1.3.36.22. Vulnerabilidades de aplicativos instalados na máquina;
1.3.37. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
1.3.38. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
1.3.38.1. Alteração de Gateway Padrão;
1.3.38.2. Alteração de subrede;
1.3.38.3. Alteração de domínio;
1.3.38.4. Alteração de servidor DHCP;
1.3.38.5. Alteração de servidor DNS;
1.3.38.6. Alteração de servidor WINS;
1.3.38.7. Alteração de subrede;
1.3.38.8. Resolução de Nome;
1.3.38.9. Disponibilidade de endereço de conexão SSL;
1.3.39. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
1.3.40. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
1.3.41. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
1.3.42. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
1.3.43. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um ser
onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
1.3.44. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigan
servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
1.3.45. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
1.3.46. Capacidade de gerar traps SNMP para monitoramento de eventos;
1.3.47. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
1.3.48. Listar em um único local, todos os computadores não gerenciados na rede;
1.3.49. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
1.3.50. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
1.3.51. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
1.3.52. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente
1.3.53. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em
1.3.54. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado i
1.3.55. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém
do computador;
1.3.56. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scar
endpoint);
1.3.57. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade n
1.3.58. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborad
informativos, de alertas ou de erros;
1.3.59. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
1.3.60. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
- Nome do vírus;
- Nome do arquivo infectado;
- Data e hora da detecção;

- Nome da máquina ou endereço IP;
- Ação realizada.

1.3.61. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
1.3.62. Capacidade de listar updates nas máquinas com o respectivo link para download
1.3.63. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;
1.3.64. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
1.3.65. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
1.3.66. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
1.3.67. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2. Estações Windows

2.1. Compatibilidade:

2.1.1. Microsoft Windows 7 Professional/Enterprise/Home SP1 x86 / x64;
2.1.2. Microsoft Windows 8 Professional/Enterprise x86 / x64;
2.1.3. Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
2.1.4. Microsoft Windows 10 Pro / Enterprise / Home / Education x86 / x64;
2.1.5. Microsoft Windows Server 2019 Essentials / Standard / Datacenter;
2.1.6. Microsoft Windows Server 2016 Essentials / Standard / Datacenter;
2.1.7. Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
2.1.8. Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
2.1.9. Microsoft Windows Server 2008 R2 Foundation / Essentials / Standard / Datacenter SP1;
2.1.10. Microsoft Windows Small Business Server 2011 Standard / Standard x64;
2.1.11. Microsoft Windows MultiPoint Server 2011 x64;

2.2. Características:

2.2.1. Deve prover as seguintes proteções:
2.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
2.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
2.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
2.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
2.2.1.5. Firewall com IDS;
2.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);
2.2.1.7. Controle de dispositivos externos;
2.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
2.2.1.9. Controle de acesso a sites por horário;
2.2.1.10. Controle de acesso a sites por usuários;
2.2.1.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
2.2.1.12. Controle de execução de aplicativos;
2.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
2.2.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
2.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaç
média ou baixa);
2.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
2.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista d
veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
2.2.6. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windo
2.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
2.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
2.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de
essa decisão e não tomar a partir da extensão do arquivo;
2.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
2.2.11. Capacidade de verificar somente arquivos novos e alterados;
2.2.12. Capacidade de verificar objetos usando heurística;
2.2.13. Capacidade de agendar uma pausa na verificação;
2.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
2.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
2.2.16. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
2.2.17. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;
2.2.18. Capacidade de verificar links inseridos em e-mails contra phishings;
2.2.19. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
2.2.20. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
2.2.21.
2.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
2.2.22.1. Perguntar o que fazer, ou;
2.2.22.2. Bloquear o e-mail;
2.2.22.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.22.2.2. Caso positivo de desinfecção:
2.2.22.2.2.1. Restaurar o e-mail para o usuário;
2.2.22.2.3. Caso negativo de desinfecção:
2.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
2.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
2.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
2.2.26. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
2.2.27. Deve ter suporte total ao protocolo Ipv6;
2.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
2.2.29. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
2.2.29.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
2.2.29.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

2.2.30. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
2.2.31. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequência perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
2.2.32. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
2.2.33. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas p bloqueadas;
2.2.34. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphish
2.2.35. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
2.2.36. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados d juntamente com as vacinas;
2.2.37. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
2.2.37.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
2.2.37.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou no rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
2.2.38. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
2.2.38.1. Discos de armazenamento locais;
2.2.38.2. Armazenamento removível;
2.2.38.3. Impressoras;
2.2.38.4. CD/DVD;
2.2.38.5. Drives de disquete;
2.2.38.6. Modems;
2.2.38.7. Dispositivos de fita;
2.2.38.8. Dispositivos multifuncionais;
2.2.38.9. Leitores de smart card;
2.2.38.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
2.2.38.11. Wi-Fi;
2.2.38.12. Adaptadores de rede externos;
2.2.38.13. Dispositivos MP3 ou smartphones;
2.2.38.14. Dispositivos Bluetooth;
2.2.38.15. Câmeras e Scanners.
2.2.39. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciam local do administrador na máquina do usuário;
2.2.40. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
2.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
2.2.42. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.
2.2.43. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
2.2.44. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);
2.2.45. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:
2.2.45.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
2.2.45.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
2.2.46. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
2.2.47. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou r
2.2.48. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de ap web;
2.2.49. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras aplicativos, dispositivos e acesso à web.
2.2.50. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.
2.2.51. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
2.2.52. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
2.2.53. Capacidade de integração com o Windows Defender Security Center.
2.2.54. Capacidade de integração com a Antimalware Scan Interface (AMSI).
2.2.55. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

3. Estações Mac OS X

3.1. Compatibilidade:

3.1.1. macOS Catalina 10.15
3.1.2. macOS Mojave 10.14
3.1.3. masOS High Sierra 10.13
3.1.4. macOS Sierra 10.12

3.2. Características:

3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificad
3.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;
3.2.3. Possuir módulo de bloqueio á ataques na rede;
3.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
3.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
3.2.6. Possibilidade de importar uma chave no pacote de instalação;
3.2.7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3.2.8. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda s
3.2.9. Deve possuir suportes a notificações utilizando o Growl;
3.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das amea média ou baixa);
3.2.11. Capacidade de voltar para a base de dados de vacina anterior;
3.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
3.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
3.2.14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
3.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação d essa decisão e não tomar a partir da extensão do arquivo;
3.2.16. Capacidade de verificar somente arquivos novos e alterados;
3.2.17. Capacidade de verificar objetos usando heurística;

3.2.18. Capacidade de agendar uma pausa na verificação;
3.2.19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
3.2.19.1. O que aplicar o que fazer, ou;
3.2.19.2. Bloquear acesso ao objeto;
3.2.19.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.2.19.2.2. Caso positivo de desinfecção:
3.2.19.2.2.1. Restaurar o objeto para uso;
3.2.19.2.3. Caso negativo de desinfecção:
3.2.19.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
3.2.20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.2.21. Capacidade de verificar arquivos de formato de email;
3.2.22. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus comando;
3.2.23. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

4. Estações de trabalho Linux

4.1. Compatibilidade:

4.1.1. Plataforma 32-bits:
4.1.1.1. Ubuntu 16.04 LTS;
4.1.1.2. Red Hat® Enterprise Linux® 6.7 Server;
4.1.1.3. CentOS 6.7;
4.1.1.4. Debian GNU / Linux 9.4 ;
4.1.1.5. Debian GNU / Linux 10;
4.1.1.6. Linux Mint 18.2;
4.1.1.7. Linux Mint 19;
4.1.1.8. GosLinux 6.6;
4.1.1.9. Mageia 4;
4.1.1.10. OS Lotos ;

4.1.2. Plataforma 64-bits:
4.1.2.1. Ubuntu 16.04 LTS;
4.1.2.2. Ubuntu 18.04 LTS;
4.1.2.3. Red Hat Enterprise Linux 6.7;
4.1.2.4. Red Hat Enterprise Linux 7.2;
4.1.2.5. Red Hat Enterprise Linux 8.0;
4.1.2.6. CentOS 6.7;
4.1.2.7. CentOS 7.2;
4.1.2.8. CentOS 8.0;
4.1.2.9. Debian GNU / Linux 9.4
4.1.2.10. Debian GNU / Linux 10.1;
4.1.2.11. OracleLinux 7.3;
4.1.2.12. OracleLinux 8;
4.1.2.13. SUSE® Linux Enterprise Server 15;
4.1.2.14. openSUSE® Leap 15;
4.1.2.15. Amazon Linux AMI
4.1.2.16. Linux Mint 18.2;
4.1.2.17. Linux Mint 19;
4.1.2.18. GosLinux 6.6
4.1.2.19. GosLinux 7.2

4.2. Características:

4.2.1. Deve prover as seguintes proteções:
4.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
4.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
4.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
4.2.5. Capacidade de criar exclusões por local, máscara e nome da ameaça;
4.2.6. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
4.2.7. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto restauração de objetos que contenham informações importantes;
4.2.8. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
4.2.9. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
4.2.9.1. Alta;
4.2.9.2. Média;
4.2.9.3. Baixa;
4.2.9.4. Recomendado;
4.2.10. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
4.2.11. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecçã infectados.
4.2.12. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
4.2.13. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
4.2.14. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação fazer essa decisão e não tomar a partir da extensão do arquivo;
4.2.15. Capacidade de verificar objetos usando heurística;
4.2.16. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
4.2.17. Possibilidade de
4.2.18. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;de administração remoto através de ferramenta na nativa GNU-Linux).

5. Servidores Windows

5.1. Compatibilidade:

5.2. Plataforma 32-bits:
5.2.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
5.2.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
5.2.3. Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior;
5.2.4. Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior;
5.3. Plataforma 64-bits
5.3.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
5.3.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
5.3.3. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter SP1 ou posterior;
5.3.4. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter SP1 ou posterior.
5.3.5. Microsoft Windows Server 2008 R2 Foundation / Standard / Enterprise / DataCenter SP1 ou posterior;
5.3.6. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter SP1 ou posterior;
5.3.7. Microsoft Small Business Server 2008 Standard / Premium
5.3.8. Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;
5.3.9. Microsoft Microsoft Small Business Server 2011 Essentials / Standard
5.3.10. Microsoft Windows MultiPoint Server 2011
5.3.11. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter / MultiPoint;
5.3.12. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
5.3.13. Microsoft Windows Server 2012 Core Standard / Datacenter;
5.3.14. Microsoft Windows Server 2012 R2 Core Standard / Datacenter;
5.3.15. Microsoft Windows Storage Server 2012;
5.3.16. Microsoft Windows Storage Server 2012 R2;
5.3.17. Microsoft Windows Hyper-V Server 2012;
5.3.18. Microsoft Windows Hyper-V Server 2012 R2;
5.3.19. Windows Server 2016 Essentials /Standard / Datacenter / MultiPoint Premium Server;
5.3.20. Windows Server 2016 Core Standard / Datacenter;
5.3.21. Windows Storage Server 2016;
5.3.22. Windows Hyper-V Server 2016;
5.3.23. Microsoft Windows Server 2019 Core / Terminal / Hyper-V
5.3.24. Windows Server IoT 2019 for Storage

5.4. Características:

5.4.1. Deve prover as seguintes proteções:
5.4.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
5.4.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;
5.4.1.3. Firewall com IDS;
5.4.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
5.4.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.4.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
5.4.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
5.4.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
5.4.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
5.4.4.3. Leitura de configurações;
5.4.4.4. Modificação de configurações;
5.4.4.5. Gerenciamento de Backup e Quarentena;
5.4.4.6. Visualização de relatórios;
5.4.4.7. Gerenciamento de relatórios;
5.4.4.8. Gerenciamento de chaves de licença;
5.4.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima);
5.4.5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
5.4.5.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
5.4.5.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou non com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
5.4.6. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que execut número máximo de processos que podem ser executados no total;
5.4.7. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede
5.4.8. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
5.4.9. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
5.4.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
5.4.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
5.4.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
5.4.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5.4.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
5.4.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
5.4.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação e essa decisão e não tomar a partir da extensão do arquivo;
5.4.17. Capacidade de verificar somente arquivos novos e alterados;
5.4.18. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compac etc.);
5.4.19. Capacidade de verificar objetos usando heurística;
5.4.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
5.4.21. Capacidade de agendar uma pausa na verificação;
5.4.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
5.4.23. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
5.4.24. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
5.4.25. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
5.4.26. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
5.4.27. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

5.4.28. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
5.4.29. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeame

6. Servidores Linux

6.1. Compatibilidade:
Plataforma 32-bits:
6.1.1.1. Ubuntu 16.04 LTS;
6.1.1.2. Red Hat® Enterprise Linux® 6.7 Server;
6.1.1.3. CentOS 6.7;
6.1.1.4. Debian GNU / Linux 9.4 ;
6.1.1.5. Debian GNU / Linux 10;
6.1.1.6. Linux Mint 18.2;
6.1.1.7. Linux Mint 19;
6.1.1.8. GosLinux 6.6;
6.1.1.9. Mageia 4;
6.1.1.10. OS Lotos ;
Plataforma 64-bits:
6.1.1.1. Ubuntu 16.04 LTS;
6.1.1.2. Ubuntu 18.04 LTS;
6.1.1.3. Red Hat Enterprise Linux 6.7;
6.1.1.4. Red Hat Enterprise Linux 7.2;
6.1.1.5. Red Hat Enterprise Linux 8.0;
6.1.1.6. CentOS 6.7;
6.1.1.7. CentOS 7.2;
6.1.1.8. CentOS 8.0;
6.1.1.9. Debian GNU / Linux 9.4
6.1.1.10. Debian GNU / Linux 10.1;
6.1.1.11. OracleLinux 7.3;
6.1.1.12. OracleLinux 8;
6.1.1.13. SUSE® Linux Enterprise Server 15;
6.1.1.14. openSUSE® Leap 15;
6.1.1.15. Amazon Linux AMI
6.1.1.16. Linux Mint 18.2;
6.1.1.17. Linux Mint 19;
6.1.1.18. GosLinux 6.6
6.1.1.19. GosLinux 7.2

6.2. Características:

6.2.1. Deve prover as seguintes proteções:
6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
6.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
6.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
6.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
6.2.2.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objet
restauração de objetos que contenham informações importantes;
6.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
6.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecçã
infectados;
6.2.3. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
6.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
6.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação d
essa decisão e não tomar a partir da extensão do arquivo;
6.2.6. Capacidade de verificar objetos usando heurística;
6.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
6.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
6.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

8. Smartphones e tablets

8.1. Compatibilidade:

8.1.1. Dispositivos com os sistemas operacionais:
8.1.1.1. Android 5.0 – 5.1.1
8.1.1.2. Android 6.0 – 6.0.1
8.1.1.3. Android 7.0 – 7.12
8.1.1.4. Android 8.0 – 8.1
8.1.1.5. Android 9.0
8.1.1.6. Android 10.0
8.1.1.7. iOS 10.0 – 10.3.3
8.1.1.8. iOS 11.0 – 11.3
8.1.1.9. iOS 12.0
8.1.1.10. iOS 13.0

8.2. Características:

8.2.1. Deve prover as seguintes proteções:
8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
8.2.1.2. Proteção contra adware e autodialers;
8.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realiz
8.2.1.4. Arquivos abertos no smartphone;

8.2.1.5. Programas instalados usando a interface do smartphone
8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
8.2.2. Deverá isolar em área de quarentena os arquivos infectados;
8.2.3. Deverá atualizar as bases de vacinas de modo agendado;
8.2.4. Deverá bloquear spams de SMS através de Black lists;
8.2.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;
8.2.6. Capacidade de desativar por política:
Wi-fi;
Câmera;
Bluetooth.
8.2.7. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
8.2.8. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
8.2.9. Deverá ter firewall pessoal (Android);
8.2.10. Capacidade de tirar fotos quando a senha for inserida incorretamente;
8.2.11. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;
8.2.12. Capacidade de enviar comandos remotamente de:
- Localizar;
- Bloquear.

8.2.13. Capacidade de detectar Jailbreak em dispositivos iOS;
8.2.14. Capacidade de bloquear o acesso a site por categoria em dispositivos;
8.2.15. Capacidade de bloquear o acesso a sites phishing ou malicioso;
8.2.16. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
8.2.17. Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;
8.2.18. Capacidade de configurar White e blacklist de aplicativos;
8.2.19. Capacidade de localizar o dispositivo quando necessário;
8.2.20. Permitir atualização das definições quando estiver em “roaming”;
8.2.21. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
8.2.22. Deve permitir verificar somente arquivos executáveis;
8.2.23. Deve ter a capacidade de desinfectar o arquivo se possível;
8.2.24. Capacidade de agendar uma verificação;
8.2.25. Capacidade de enviar URL de instalação por e-mail;
8.2.26. Capacidade de fazer a instalação através de um link QRCode;
8.2.27. Capacidade de executar as seguintes ações caso a desinfecção falhe:
- Deletar;
- Ignorar;
- Quarentenar;
- Perguntar ao usuário.

9. Gerenciamento de dispositivos móveis (MDM)

9.1. Compatibilidade:

Dispositivos com os sistemas operacionais:
9.1.1.1. Android 5.0 – 5.1.1
9.1.1.2. Android 6.0 – 6.0.1
9.1.1.3. Android 7.0 – 7.12
9.1.1.4. Android 8.0 – 8.1
9.1.1.5. Android 9.0
9.1.1.6. Android 10.0
9.1.1.7. iOS 10.0 – 10.3.3
9.1.1.8. iOS 11.0 – 11.3
9.1.1.9. iOS 12.0
9.1.1.10. iOS 13.0

9.1.2. Softwares de gerência de dispositivos:
9.1.2.1. VMWare AirWatch 9.3;
9.1.2.2. MobileIron 10.0;
9.1.2.3. IBM Maas360 10.68;
9.1.2.4. Microsoft Intune 1908;
9.1.2.5. SOTI MobiControl 14.1.4 (1693);

9.2. Características:

9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
9.2.2. Capacidade de ajustar as configurações de:
9.2.2.1. Sincronização de e-mail;
9.2.2.2. Uso de aplicativos;
9.2.2.3. Senha do usuário;
9.2.2.4. Criptografia de dados;
9.2.2.5. Conexão de mídia removível.
9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS;
9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS;
9.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
9.2.8. Possibilidade de exigir senha para abrir aplicações instaladas em container;
9.2.9. Deve permitir que o usuário utilize autenticação do Active Directory para abrir aplicações em container;
9.2.10. Deve permitir que uma senha seja digitada a cada x(minutos) para continuar utilizando uma aplicação em container;
9.2.11. Deve permitir a criptografia de dados salvos pelas aplicações em container;
9.2.12. Permitir sincronização com perfil do “Touch Down”;
9.2.13. Capacidade de desinstalar remotamente o antivírus do dispositivo;
9.2.14. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
9.2.15. Capacidade de sincronizar com Samsung Knox;

10. Criptografia

10.1. Compatibilidade

10.1.1. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
10.1.2. Microsoft Windows 8 Enterprise x86/x64;
10.1.3. Microsoft Windows 8 Pro x86/x64;
10.1.4. Microsoft Windows 8.1 Pro x86/x64;
10.1.5. Microsoft Windows 8.1 Enterprise x86/x64;
10.1.6. Microsoft Windows 10 Pro / Enterprise / Home / Education x86 / x64;

10.2. Características

10.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimer
10.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
10.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
10.2.4. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;
10.2.5. Permitir criar vários usuários de autenticação pré-boot;
10.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
10.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
10.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
10.2.7.2. Criptografar todos os arquivos individualmente;
10.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
10.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
10.2.8. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem est
máquinas gerenciadas pela mesma console de maneira transparente para os usuários;
10.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
10.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
10.2.11. Verifica compatibilidade de hardware antes de aplicar a criptografia;
10.2.12. Possibilita estabelecer parâmetros para a senha de criptografia;
10.2.13. Bloqueia o reuso de senhas;
10.2.14. Bloqueia a senha após um número de tentativas pré-estabelecidas;
10.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
10.2.16. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
10.2.17. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
10.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
10.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
10.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados;
10.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
10.2.22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
10.2.23. Capacidade de deletar arquivos de forma segura após a criptografia;
10.2.24. Capacidade de criptografar somente o espaço em disco utilizado;
10.2.25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
10.2.26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
10.2.27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
10.2.28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
10.2.29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
10.2.30. Capacidade de fazer “Hardware encryption”;

11. Gerenciamento de Sistemas

11.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computad
11.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
11.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
11.4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualiza
maneira transparente para os usuários;
11.5. Capacidade de gerenciar licenças de softwares de terceiros;
11.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
11.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informan
encontra, service tag, número de identificação e outros;
11.8. Possibilita fazer distribuição de software de forma manual e agendada;
11.9. Suporta modo de instalação silenciosa;
11.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
11.11. Possibilita fazer a distribuição através de agentes de atualização;
11.12. Utiliza tecnologia multicast para evitar tráfego na rede;
11.13. Possibilita criar um inventário centralizado de imagens;
11.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
11.15. Suporte a WakeOnLan para deploy de imagens;
11.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
11.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no compo
11.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
11.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
11.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
11.21. Permite baixar atualizações para o computador sem efetuar a instalação
11.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações in
11.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
11.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
11.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
11.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
11.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores co
administrador;
11.28. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;
11.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
11.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

ANEXO II – DO TERMO DE REFERÊNCIA

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Os abaixo-assinados, de um lado a _____, CNPJ nº _____/_____, situada na cidade de _____, à Rua: _
_____, doravante denominada CONTRATANTE, e de outro lado _____, CNPJ nº _____/_____, situada na cid
_____, à Rua: _____, bairro _____, doravante denominada CONTRATADA, tem entre si justa e acertada, a celebra
COMPROMISSO, SIGILO E CONFIDENCIALIDADE, através do qual a CONTRATADA aceita não divulgar sem autorização prévia e formal segredos e inform
da _____ e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:
PRIMEIRA – A CONTRATADA reconhece que em razão das suas atividades profissionais, estabelece contato com informações sigilosas, que devem ser entendic
informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios Cola
expressa e escrita autorização da _____.
SEGUNDA - As informações, exemplificadas abaixo, devem receber o tratamento de confidencialidade adequado, de acordo com o seu nível de classificação.
1. Programas de computador, suas listagens, documentação, artefatos diversos, código fonte e código objeto;
2. Toda a informação relacionada a programas existentes ou em fase de desenvolvimento no âmbito da, inclusive fluxogramas, estatísticas, especificações, avaliaç
de dados, artefatos diversos e versões “beta” de quaisquer programas;
3. Documentos, informações e dados armazenados de atuação consultiva e contenciosa, de estratégias ou demais dados e/ou informações de caráter sigiloso ou res
4. Metodologia, projetos e serviços utilizados;
5. Números e valores financeiros.
TERCEIRA – A CONTRATADA reconhece que a lista acima é meramente exemplificativa e ilustrativa e que outras hipóteses de confidencialidade que já existam
futuro devem ser mantidas sob segredo. Em caso de dúvida acerca da confidencialidade de determinada informação a CONTRATADA deve tratar a mesma sob si
formalmente, a tratá-la de forma diferente pela CONTRATANTE.
QUARTA – A CONTRATADA reconhece que, no seu desligamento definitivo da _____, deverá entregar à CONTRATANTE todo e qualquer material de proprie
pessoais envolvendo matérias sigilosas relacionadas com a _____, registros de documentos de qualquer natureza que tenham sido usados, criados ou estado sob se
também assume o compromisso de não utilizar qualquer informação adquirida quando de suas atividades para a _____.
QUINTA – A CONTRATADA deve assegurar que todos os seus colaboradores guardarão sigilo sobre as informações que porventura tiverem acesso, mediante o c
Termo próprio a ser firmado entre a CONTRATADA e seus colaboradores, e que os mesmos comprometer-se-ão a informar, imediatamente, ao seu superior hierár
regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional.
Parágrafo Primeiro: A coleta dos Termos de Sigilo de seus colaboradores não exime a CONTRATADA das penalidades por violação das regras por parte de seus c
Parágrafo segundo: A CONTRATADA deverá fornecer cópia de todos os termos firmados com seus colaboradores à _____ no prazo de 10 dias após assinatura d
Parágrafo Terceiro: Sempre que um colaborador for admitido, A CONTRATADA deverá fornecer cópia dos novos termos firmados no prazo de 2 dias após assina
SEXTA - O atendimento deste TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE, bem como da das Diretrizes Básicas da Política de Seguranç
incorporados formalmente ao contrato de trabalho dos funcionários da CONTRATADA que prestarem serviços à _____.
SÉTIMA – A CONTRATADA deverá seguir a Política de Segurança da Informação definida pela CONTRATANTE.
OITAVA - O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização civil e criminal, de acordo com a legislação vigente.

Em,_____de _____de 20___.

_____
Responsável pelo Contrato - CONTRATANTE

_____
Responsável pelo Contrato - CONTRATADA

ANEXO II

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

ANEXO II

VTECH SEGURANÇA DE INFORMAÇÃO
PROPOSTA DE PREÇOS
PROCESSO Nº: 006.0409.2021.0039114-85
PREGÃO ELETRÔNICO 04/2022

22/03/2022

Cliente:	**PROCURADORIA GERAL DO ESTADO DA BAHIA – PGE**
Pregão Eletrônico:	Pregão Eletrônico 04/2022 Processo Administrativo nº 006.0409.2021.0039114-85
Endereçado à:	Comissão Licitação
Referência do objeto:	Proposta de renovação de licença/garantia das licenças de software antivírus utilizadas nas estações de trabalho e servidores da PGE com garantia de 36 meses, contendo serviço de configuração/atualização e suporte on site.

QUEM É A VTECH?

A VTECH é uma empresa focada em Segurança da Informação e Comunicação, que fornece soluções inovadoras em TI visando atender aos nossos clientes com celeridade, flexibilidade e inovação, sempre prezando pela qualidade de seus serviços.

Atuando em todo o território nacional, oferecemos soluções para proteção de seus negócios com tecnologia de ponta com o propósito de garantir segurança e privacidade total no mundo digital.

OBJETO

A proposta tem por finalidade de renovação de licença/garantia das licenças de software antivírus utilizadas nas estações de trabalho e servidores da PGE com garantia de 36 meses, contendo serviço de configuração/atualização e suporte on site.

LOTE ÚNICO				
ITEM	**Descrição**	**Unidade de Fornecimento (UF)**	**Quantitativo**	**Cronograma/Prazo**
1	RENOVAÇÃO DE LICENÇA DE USO DE SOFTWARE, *Kaspersky Endpoint Security for Business advanced*, com suporte e atualização. Para estações de trabalho e servidores pelo período de 36 (trinta e seis) meses Código SIMPAS: 02.81.23.00000301-8	**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

VTECH SEGURANÇA DE INFORMAÇÃO
PROPOSTA DE PREÇOS
PROCESSO Nº: 006.0409.2021.0039114-85
PREGÃO ELETRÔNICO 04/2022
22/03/2022

LOCAL DA PRESTAÇÃO DE SERVIÇO Os serviços serão prestados na sede da Procuradoria Geral do Estado, situada na 3ª Av. Centro Administrativo da Bahia, 370, CAB, Salvador – BA, CEP: 41.745-005 - Salvador Bahia.

PERÍODO DE GARANTIA (OU DE LICENCIAMENTO)

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 deve 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.

Será entregue e instalado pelos técnicos da VTECH, na quantidade e características especificadas e dentro do prazo fixado e respeitando os termos estabelecidos no edital;

O produto estará licenciado em nome da PGE, sendo que o suporte, a manutenção e suas atualizações (upgrade e update) deverão ocorrer sem ônus para este Órgão;
Acesso telefônico 08h/dia, 5 dias da semana;

SUPORTE TÉCNICO E ACORDO DE NÍVEL DE SERVIÇO

OBJETIVO:

Atender às necessidades da PGE para suporte técnico do antivírus, com o objetivo de proteger a rede corporativa e aumentar o nível de conformidade com a política de segurança.

EQUIPE TÉCNICA:

Composta de técnicos capacitados pelo fabricante do software fornecido, e preparada para dar todo o suporte técnico e ajuda necessária para maximizar os benefícios oferecidos pelo software, aumentando a sua performance.

SUPORTE TÉCNICO:

O suporte técnico ao produto será prestado 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;

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

Será executados pela VTECH contratada serviços de Consultoria, Instalação e Configuração para uso da solução contratada com supervisão da equipe técnica da PGE;

Será executada pela VTECH 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;

Pregão Eletrônico 04/22 nº fls. 36/50

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO
PROPOSTA DE PREÇOS
PROCESSO Nº: 006.0409.2021.0039114-85
PREGÃO ELETRÔNICO 04/2022
22/03/2022

A VTECH preservará todo ambiente computacional existente, de forma a manter a integridade dos dados, aplicativos e sistemas operacionais em funcionamento;

A VTECH preparará o ambiente de modo a operar conforme o estabelecido no plano de otimização de recursos, rotinas, procedimentos e processos;

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;

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

O Prazo de execução dos serviços de Instalação, Configuração e 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;

A VTECH realizará 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;

Todo suporte será prestado por técnicos capacitados pelo fabricante;

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

O suporte técnico será prestado nas seguintes formas:

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

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 8 (oito) horas por dia, 5 (cinco) dias por semana, para este tipo de atendimento;

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;

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

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO
PROPOSTA DE PREÇOS
PROCESSO Nº: 006.0409.2021.0039114-85
PREGÃO ELETRÔNICO 04/2022
22/03/2022

acionar o atendimento, no local designado pela PGE, de acordo com o nível de serviço acordado. O suporte prestado pela empresa terá chamados ilimitados;

O atendimento No Local (on site) deve ser provido na PGE, no seguinte endereço: 2ª Avenida Centro Administrativo da Bahia, 250 - CAB, Salvador - BA, 41745-003

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

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

Entende-se por início do atendimento a hora do contato do técnico de suporte da Contratada com a equipe da Contratante;
Entende-se por término de atendimento a disponibilidade do produto para uso em perfeitas ESTADO DA BAHIA condições de funcionamento no local onde está instalado;

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

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

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

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;

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

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

ACORDO DE NÍVEL DE SERVIÇO (ANS):

A VTECH possui Central de Atendimento (contato telefônico, sitio na Internet e email) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 8 (oito) horas por dia, 5 (cinco) dias por semana;

A VTECH prestará serviços de suporte técnico 8 horas por dia, 5 dias por semana, na cidade de Salvador (BA), relativos a prestação do serviço objeto deste Termo de Referência, sem ônus para a Contratante;

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

Pregão Eletrônico 04/22 nº fls. 38/50

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO
PROPOSTA DE PREÇOS
PROCESSO N°: 006.0409.2021.0039114-85
PREGÃO ELETRÔNICO 04/2022
22/03/2022

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.

A VTECH fará análises dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe da CONTRATANTE.

A VTECH apresentará relatório contendo as ações adotadas para a solução do problema.

A VTECH disponibilizará 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.

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;

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.

Níveis de Serviço e Tempo Esperados:

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

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 d

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

VTECH COMERCIO, SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA EIRELI
Avenida Santos Dumont, 4487, Km 3,5, Loja 157, Shopping Passeio Norte, Estrada do Coco, Lauro de Freitas, Bahia, CEP 42.702-400

Pregão Eletrônico 04/22 nº fls. 39/50

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO
PROPOSTA DE PREÇOS
PROCESSO Nº: 006.0409.2021.0039114-85
PREGÃO ELETRÔNICO 04/2022
22/03/2022

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
On Site	Término atendimento	2 horas	4 horas	72 horas
Telefone, e-mail e web	Início atendimento	-	-	24 horas
	Término atendimento	-	-	72 horas

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;

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.

A VTECH disponibilizará 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;

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;

A VTECH prestará 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.

A VTECH ainda realizará os seguintes suportes proativos:

Duas 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

Pregão Eletrônico 04/22 nº fls. 40/50

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO
PROPOSTA DE PREÇOS
PROCESSO N°: 006.0409.2021.0039114-85
PREGÃO ELETRÔNICO 04/2022
22/03/2022

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.

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

Fatos Diretos sobre a Kaspersky

- A maior empresa privada de antimalware do mundo
- Crescimento sem precedentes, oito vezes maior que a média do setor

- Crescimento sem precedentes, cinco vezes maior que a média do setor
- Mais de 300 milhões de usuários em todo o mundo
- 50.000 novos sistemas adicionados por semana

Por que a Kaspersky?

A Kaspersky Lab fornece a proteção mais imediata contra ameaças à segurança da TI, que incluem vírus, spyware, crimeware, hackers, phishing e spam. Os nossos produtos fornecem taxas de detecção superiores e o menor tempo de resposta a surtos do setor para usuários domésticos, pequenas e médias empresas, grandes corporações e o ambiente de computação móvel. A tecnologia da Kaspersky® também é usada em todo o mundo em produtos e serviços dos líderes do setor no fornecimento de soluções de segurança de TI.

Nós investimos todos os nossos recursos e conhecimento para impedir a disseminação dessas ameaças. Nós ajudamos a informar a comunidade envolvida sobre as práticas recomendáveis a fim de assegurar a melhor segurança online possível.

O sucesso de nossa missão resultou no destaque da Kaspersky Lab como a maior empresa privada de antimalware do mundo. Fundada em 1997, a empresa fornece seus produtos e tecnologias para o setor e os consumidores em praticamente todos os países do mundo. Atualmente, mais de 300 milhões de usuários em todo o mundo estão protegidos por nossas tecnologias. E, todas as semanas, adicionamos mais de 50.000 novos sistemas.

Pregão Eletrônico 04/22 nº fls. 41/50

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO
PROPOSTA DE PREÇOS
PROCESSO N°: 006.0409.2021.0039114-85
PREGÃO ELETRÔNICO 04/2022
22/03/2022

DOS PREÇOS

LOTE ÚNICO

Item	Descrição	UF	Qtd	Valor Unitário (R$	Valor Total (R$)
01	Renovação de Licença de uso de Software, Kaspersky Endpoint Security for Business ADVANCED, com suporte e atualização. Para estações de trabalho e servidores pelo período de 36 (trinta e seis) meses Modelo/Versão: Kaspersky Endpoint Security for Business **ADVANCED** Fabricante: Kaspersky Código SIMPAS: 02.81.23.00000301-8	Und	1.000	R$ 162,94	R$ 162.940,
	Valor total		R$ 162.940,00		

Valor total da proposta R$ 162.940,00 (cento e sessenta e dois mil novecentos e quarenta reais).

A validade desta proposta é de 60 (sessenta dias), a partir da sua apresentação

Prazo de entrega: até 30 (trinta) dias, contados a partir da assinatura do contrato ou instrumento equivalente;

A VTECH garante e comprova ser representante do fabricante do software ofertado, mediante apresentação de declaração do fabricante.

A proposta prever e especificar o período de garantia de 36 meses com atendimento ON-SITE em até 4 horas.

A proposta prever e especificar a transferência de conhecimento à equipe da PGE, de toda solução ofertada com carga horária mínima de 20 horas;

Prazo de Garantia, licenciamento: de 36 (trinta e seis) meses, com suporte técnico e atualização.

No valor da proposta estão contempladas todas e quaisquer despesas necessárias ao 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 Contratada, como também fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, tributos, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela Contratada das obrigações

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO
PROPOSTA DE PREÇOS
PROCESSO N°: 006.0409.2021.0039114-85
PREGÃO ELETRÔNICO 04/2022
22/03/2022

Lauro de Freitas, Bahia 22 de março de 2022

NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520

Assinado de forma digital por NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520
Dados: 2022.03.22 10:59:40 -03'00'

Natasha de Matos Oliveira Araújo
CPF: 628.604.105-20
RG: 04.705.945-19
Endereço Postal: Avenida Santos Dumont, 4487, Km 3,5, Loja 157, Shopping Passeio Norte, Estrada do Coco, Lauro de Freitas, Bahia, CEP 42.702-400.
Endereço Eletrônico: Comercial@vtechti.com.br / Natasha@vtechti.com.br
Razão social: VTECH COMERCIO, SERVICOS E EQUIPAMENTOS DE INFORMATICA EIRELI
CNPJ: 22.122.370/0001-34
Cargo: Diretora Geral
Tel: (71)3289-0643 | 71 9625-5980
Insc. Municipal: 001.001.7482 | Insc. Estadual: 123.555.216 ME
Banco do Bradesco Agência 0592-4, Conta Corrente: 11.304-2

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO
PROPOSTA DE PREÇOS
PROCESSO Nº: 006.0409.2021.0039114-85
PREGÃO ELETRÔNICO 04/2022
22/03/2022

Lauro de Freitas, Bahia 22 de março de 2022

NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520
Assinado de forma digital por NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520
Dados: 2022.03.22 10:59:40 -03'00'

Natasha de Matos Oliveira Araújo
CPF: 628.604.105-20
RG: 04.705.945-19
Endereço Postal: Avenida Santos Dumont, 4487, Km 3,5, Loja 157, Shopping Passeio Norte, Estrada do Coco, Lauro de Freitas, Bahia, CEP 42.702-400.
Endereço Eletrônico: Comercial@vtechti.com.br / Natasha@vtechti.com.br
Razão social: VTECH COMERCIO, SERVICOS E EQUIPAMENTOS DE INFORMATICA EIRELI
CNPJ: 22.122.370/0001-34
Cargo: Diretora Geral
Tel: (71)3289-0643 | 71 9625-5980
Insc. Municipal: 001.001.7482 | Insc. Estadual: 123.555.216 ME
Banco do Bradesco Agência 0592-4, Conta Corrente: 11.304-2

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO

À PROCURADORIA GERAL DO ESTADO

Modalidade de Licitação	Número
Pregão Eletrônico	**04/2022**

Processo administrativo: 006.0409.2021.0039114-8

DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA E DE INEXISTENCI DE IMPEDIMENTO A PARTICIPAÇÃO NO CERTAME

Natasha de Matos Oliveira Araújo, RG n° 04.705.945-19, CPF n° 628.604.105-20, con representante devidamente constituída da VTECH Comercio, Serviços e Equipamentos Informática EIRELI, CNPJ n° 22.122.370/0001-34, situada na Avenida Santos Dumont, 448 Km 3,5, Loja 157, Shopping Passeio Norte, Estrada do Coco, CEP 42.702-400 - Lauro de Freit – Bahia, doravante denominada LICITANTE, para fins de participação no certame licitató acima identificado, declaro, sob as penas da lei, em especial o art. 299 do Código Pen Brasileiro, que:

(a) a proposta apresentada para participar desta licitação foi elaborada de manei independente por mim e o conteúdo da proposta não foi, no todo ou em parte, direta indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou fato desta licitação, por qualquer meio ou por qualquer pessoa;

(b) a intenção de apresentar a proposta elaborada para participar desta licitação não f informada, discutida ou recebida de qualquer outro participante potencial ou de fato des licitação, por qualquer meio ou por qualquer pessoa;

(c) que não tentei, por qualquer meio ou por qualquer pessoa, influir na decisão de qualqu outro participante potencial ou de fato desta licitação quanto a participar ou não dela;

(d) que o conteúdo da proposta apresentada para participar desta licitação não será, no todo em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro participan potencial ou de fato desta licitação antes da adjudicação do objeto;

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO

(e) que o conteúdo da proposta apresentada para participar desta licitação não foi, no todo o em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer integrante o órgão licitante antes da abertura oficial das propostas; e

(f) que estou plenamente ciente do teor e da extensão desta declaração e que detenho plen poderes e informações para firmá-la.

Declaro, ainda, para os efeitos art. 299 do Código Penal Brasileiro, não estar sujeito a hipóteses de impedimento de participação elencadas nos arts. 18 e 125 da Lei estadual n 9.433/05, quais sejam:

Art. 18 - Não poderá participar, direta ou indiretamente, da licitação, da execução de obras o serviços e do fornecimento de bens a eles necessários: I - o autor do projeto, básico o executivo, pessoa física ou jurídica; II - a empresa responsável, isoladamente ou em consórci pela elaboração do projeto básico ou executivo ou da qual o autor do projeto seja dirigent gerente, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto o controlador, responsável técnico, subordinado ou subcontratado;
III - servidor ou dirigente do órgão ou entidade contratante ou responsável pela licitação; IV demais agentes públicos, assim definidos no art. 207 desta Lei, impedidos de contratar com Administração Pública por vedação constitucional ou legal.

§ 1º - É permitida a participação do autor do projeto ou da empresa, a que se refere o inciso deste artigo, na licitação ou na execução da obra ou serviço, como consultor ou técnico, na funções de fiscalização, supervisão ou gerenciamento, exclusivamente a serviço o Administração interessada.
§ 2º - O disposto neste artigo não impede a licitação ou contratação de obra ou serviço qu

inclua, como encargo do contratado ou pelo preço previamente fixado pela Administração, elaboração do projeto executivo.

§ 3º - Considera-se participação indireta, para os fins do disposto neste artigo, a existência qualquer vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou parentesco até o 3º grau entre o autor do projeto, pessoa física ou jurídica, e o licitante ou

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO

responsável pelos serviços, fornecimentos e obras, incluindo-se o fornecimento de bens serviços a estes necessários.

§ 4º - Aplica-se o disposto no parágrafo anterior aos membros da comissão de licitação.

Art. 125 - É vedado ao agente político e ao servidor público de qualquer categoria, natureza condição, celebrar contratos com a Administração direta ou indireta, por si ou com representante de terceiro, sob pena de nulidade, ressalvadas as exceções legais.

Parágrafo único - Não se inclui na vedação deste artigo a prestação de serviços em caráter eventual, de consultoria técnica, treinamento e aperfeiçoamento, bem como a participação e comissões examinadoras de concursos, no âmbito da Administração Pública.

Lauro de Freitas - BA, 22 de março de 2022

NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520

Assinado de forma digital por NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520
Dados: 2022.03.17 11:24:40 -03'00'

Natasha de Matos Oliveira Araújo
RG: 04.705.945-19
CPF: 628.604.105-20

Comercial@vtechti.com.br
Diretora
VTECH COMERCIO, SERVIÇOS E EQUIPAMENTOS DE INFORMATICA EIRELI
CNPJ: 22.122.370/0001-34
Tel: (71)3289-0643

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO

À PROCURADORIA GERAL DO ESTADO

Modalidade de Licitação	Número
Pregão Eletrônico	**04/2022**

Processo administrativo: 006.0409.2021.0039114-8

DECLARAÇÃO DE PLENO CONHECIMENTO E DE VERACIDADE DOS DOCUMENTOS

Em cumprimento ao art. 120, II da Lei estadual no 9.433/05 e ao art. 18, §4o do Decreto r
19.896/20, e em face do quanto disposto no art. 184, inc. V, e no art. 195 da Lei estadual r
9.433/05, declaro:

(X) o pleno conhecimento e atendimento às exigências de habilitação.

[ou]

[exclusivamente para microempresas e empresas de pequeno por

beneficiárias da Lei Complementar nº 123/0

( ) o pleno conhecimento e atendimento às exigências de habilitação, ressalvada, na forn
do §1º do art.43 da Lei complementar nº 123/06, a existência de restrição fiscal e/ou trabalhist

Declaro, ainda, a veracidade dos documentos por mim apresentados, sob as penas da lei.

Lauro de Freitas - BA, 22 de março de 2022

NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520 Assinado de forma digital por NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520 Dados: 2022.03.17 11:26:45 -03'00'

Natasha de Matos Oliveira Araújo
RG: 04.705.945-19
CPF: 628.604.105-20
Comercial@vtechti.com.br
Diretora
VTECH COMERCIO, SERVIÇOS E EQUIPAMENTOS DE INFORMATICA EIRELI
CNPJ: 22.122.370/0001-34
Tel: (71)3289-0643

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

VTECH SEGURANÇA DE INFORMAÇÃO

À PROCURADORIA GERAL DO ESTADO

Modalidade de Licitação	Número
Pregão Eletrônico	**04/2022**

Processo administrativo: 006.0409.2021.0039114-8

DECLARAÇÃO DE ENQUADRAMENTO (LEI COMPLEMENTAR no 123/06)

Para os efeitos do tratamento diferenciado da Lei Complementar no 123/06, declaramos: que estamos enquadrados, na data designada para o início da sessão pública da licitação, r condição

( ) de microempresa [ou] (X) de empresa de pequeno porte

e que não estamos incursos nas vedações a que se reporta o §4o do art. 3o da L Complementar no 123/06.

Lauro de Freitas - BA, 22 de março de 2022

NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520 Assinado de forma digital por NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520 Dados: 2022.03.17 11:26:05 -03'00'

Natasha de Matos Oliveira Araújo
RG: 04.705.945-19
CPF: 628.604.105-20
Comercial@vtechti.com.br
Diretora
VTECH COMERCIO, SERVIÇOS E EQUIPAMENTOS DE INFORMATICA EIRELI
CNPJ: 22.122.370/0001-34
Tel: (71)3289-0643

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

Ministério do Desenvolvimento, Indústria e Comércio Exterior
Secretaria de Comércio e Serviços
Departamento Nacional de Registro do Comércio
JUNTA COMERCIAL DO ESTADO DA BAHIA

DECLARAÇÃO DE REENQUADRAMENTO DE ME PARA EPP

A empresa VTECH COMÉRCIO, SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA - EIRELI ME registrado na Junta Comercial em 25/03/2015, NIRE: 29600068263, CNPJ: 22122370000134, estabelecida na(o) AVENIDA SANTOS DUMONT, 4487, KM 3,5 LOJA 157 SHOPPING PASSEIO NORTE, ESTRADA DO COCO, LAURO DE FREITAS, BA, CEP 42700000, requer a Vossa Senhoria o arquivamento do presente instrumento e declara, sob as penas da lei, que se reenquadra da condição de MICROEMPRESA PARA EMPRESA DE PEQUENO PORTE, nos termos da Lei Complementar nº 123, de 14/12/2006.

Código do ato: 307
Descrição do Ato: Reenquadramento de MICROEMPRESA COMO EMPRESA DE PEQUENO PORTE

LAURO DE FREITAS/BA, 16 de agosto de 2017.

NATASHA DE MATOS OLIVEIRA ARAUJO

Para uso exclusivo da Junta Comercial

DEFERIDO EM 23/08/2017

Roberto Ramos
Port. 086/13
Sede

JUNTA COMERCIAL DO ESTADO DA BAHIA
CERTIFICO O REGISTRO EM: 23/08/2017 SOB Nº: 97690952
JUCEB Protocolo: 17/391510-8, DE 22/08/2017
Empresa:29 6 0006826 3
VTECH COMÉRCIO, SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA - EIRELI ME
HÉLIO PORTELA RAMOS
SECRETARIO-GERAL

Requerimento: 81700000736364

NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520 Assinado NATASHA ARAUJO:6 Dados: 20 -03'00'

Pregão Eletrônico 04/22 nº fls. 49/50

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

Ministério do Desenvolvimento, Indústria e Comércio Exterior
Secretaria de Comércio e Serviços
Departamento Nacional de Registro do Comércio
JUNTA COMERCIAL DO ESTADO DA BAHIA

DECLARAÇÃO DE REENQUADRAMENTO DE ME PARA EPP

A empresa VTECH COMÉRCIO, SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA - EIRELI ME registrado na Junta Comercial em 25/03/2015, NIRE: 29600068263, CNPJ: 22122370000134, estabelecida na(o) AVENIDA SANTOS DUMONT, 4487, KM 3,5 LOJA 157 SHOPPING PASSEIO NORTE, ESTRADA DO COCO, LAURO DE FREITAS, BA, CEP 42700000, requer a Vossa Senhoria o arquivamento do presente instrumento e declara, sob as penas da lei, que se reenquadra da condição de MICROEMPRESA PARA EMPRESA DE PEQUENO PORTE, nos termos da Lei Complementar nº 123, de 14/12/2006.

Código do ato: 307
Descrição do Ato: Reenquadramento de MICROEMPRESA COMO EMPRESA DE PEQUENO PORTE

LAURO DE FREITAS/BA, 16 de agosto de 2017.

NATASHA DE MATOS OLIVEIRA ARAUJO

Para uso exclusivo da Junta Comercial

DEFERIDO EM 23/08/2017

Roberto Ramos
Port. 086/13
Sede

JUNTA COMERCIAL DO ESTADO DA BAHIA
JUCEB CERTIFICO O REGISTRO EM: 23/08/2017 SOB Nº: 97690952
Protocolo: 17/391510-8, DE 22/08/2017
Empresa:29 6 0006826 3
VTECH COMÉRCIO, SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA - EIRELI ME
HÉLIO PORTELA RAMOS
SECRETARIO-GERAL

Requerimento: 81700000736364

NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520 Assinado NATASHA ARAUJO:6 Dados: 20 -03'00'

Pregão Eletrônico 04/22 nº fls. 49/50

ESTADO DA BAHIA
PROCURADORIA GERAL DO ESTADO

Documento assinado eletronicamente por **Natasha de Matos Oliveira Araújo**, **Representante Legal da Empresa**, em 07/04/2022, às 14:17, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

Documento assinado eletronicamente por **Paulo Moreno Carvalho**, **Procurador Geral do Estado**, em 11/04/2022, às 16:54, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

Documento assinado eletronicamente por **Jucilene Meneses do Sacramento Bispo**, **Assistente de Procuradoria**, em 11/04/2022, às 17:16, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

A autenticidade deste documento pode ser conferida no site https://seibahia.ba.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **00045380204** e o código CRC **5757D6B3**.

Referência: Processo nº 006.7550.2022.0012628-16 SEI nº 00045380204

DIÁRIO OFICIAL
República Federativa do Brasil - Estado da Bahia
SALVADOR, **TERÇA-FEIRA**, 12 DE ABRIL DE 2022 - ANO CVI - Nº 23.394

RECURSOS

SECRETARIA DA EDUCAÇÃO

NOTIFICAÇÃO ADMINISTRATIVA Nº 28/2022
A Comissão Processante Local, instituída pela Portaria nº 634/2021, de 04 de março de 2021, com fulcro no art. 123 da Lei Estadual n° 12.209/11, resolve NOTIFICAR a empresa **Maria das Graças de Jesus**, inscrita no CNPJ sob o nº 26.144.583/0001-18, para que, no prazo de 30 (trinta) dias, contados a partir da publicação deste ato, efetue o pagamento do valor de R$ 284,40 (duzentos e oitenta e quatro reais e quarenta centavos), respectivo a penalidade de multa imputada nos autos do processo sancionatório SEI nº 011.5558.2020.0031212-51. Advertimos que o prazo para impugnação dos cálculos relativos ao valor da multa acima indicado é de 10 (dez) dias, contados a partir da publicação deste ato. Informamos a possibilidade de solicitação de parcelamento da dívida, que deverá ser apresentada formalmente perante a esta Comissão Processante Local, requerimento que será apreciado nos termos do art. 50 do Decreto Estadual n° 15 805/14. Salientamos que o não pagamento no prazo acima referido importará em inscrição do débito em Divida Ativa Não Tributária - DANT, pela Procuradoria Geral do Estado - PGE, nos termos da Lei Estadual n° 13.446/15. Fica franqueada vistas ao processo SEI nº 011.5558.2020.0031212-51, mediante solicitação prévia, que deverá ser remetida para o endereço eletrônico: comissaoprocessante.sec@educacao.ba.gov.br. Salvador, 07 de abril de 2022. **Lívia Silva** - **Presidente da Comissão Processante Local - SEC**

SECRETARIA DA FAZENDA

Agência de Fomento do Estado da Bahia S/A – DESENBAHIA

JULGAMENTO DO RECURSO - MODO DE DISPUTA ABERTO ELETRÔNICO Nº 011/2021 - DESENBAHIA
O Diretor de Administração e Finanças, em exercício, no uso de suas atribuições, com fundamento no Art. 53 do Regulamento Interno de Licitações, Contratos e Procedimentos Auxiliares à Licitação da Desenbahia, com fulcro no Parecer nº GJU - RCE - 69/2021 e no Parecer da Procuradoria Geral do Estado - Parecer nº PGE - NAE - 005/2022, decide **NEGAR PROVIMENTO AOS RECURSOS** interpostos pelas licitantes, GESTALT VIGILÂNCIA PATRIMONIAL LTDA e MAP SERVIÇO DE SEGURANÇA EIRELI. Mantenha-se a classificação do vencedor, REI SEGURANÇA PATRIMONIAL EIRELI. Salvador, Bahia.

SECRETARIA DO TRABALHO, EMPREGO, RENDA E ESPORTE

Superintendência dos Desportos do Estado da Bahia – SUDESB

COMUNICADO DE INTERPOSIÇÃO DE RECURSO - CONCORRÊNCIA PÚBLICA Nº 002/2021 (SETRE/SUDESB)
O Presidente da Comissão de Licitação da SUDESB comunica as empresas participantes da licitação supracitada, que a empresa **BV Construções**, **Serviços e Incorporações Ltda**, impetrou recurso, tempestivamente quanto ao resultado final do Julgamento da Habilitação no lote VII, ficando todos os interessados notificados da interposição do referido recurso, o qual poderá ser impugnado no prazo de **05 (cinco) dias úteis**, a partir desta publicação, estando franqueada vista a documentação. Salvador/BA. 11/04/2022. Osvan Rodrigo dos Santos Ramos - Presidente da Comissão.

CONTRATOS

CASA MILITAR

RESUMO DE CONTRATO n.º CMG/007/2022

PREGÃO ELETRÔNICO n.º CMG/005/2022 - **CONTRATO n.º** CMG/007/2022 - **CONTRATANTE:** Estado da Bahia / Casa Militar do Governador - **CONTRATADA:** City Serviços e Transportes Especializados EIRELI, CNPJ nº 24.400.398/0001-11- **OBJETO**: Prestação de serviços de lavagem completa de veículo automotor, leve e semi-leve, parte interna e externa- **VALOR ANUAL:** R$ 48.672,00 (quarenta e oito mil seiscentos e setenta e dois reais). - **DOTAÇÃO ORÇAMENTÁRIA**: Atividade: 2114 - Elemento de Despesa: 3.3.90.39 - Fonte: 0.100.000000 / 0.300.000000 - **PRAZO DE DURAÇÃO:** 12 (doze) meses, de 12/04/2022 a 11/04/2023 - **REGIME DE EXECUÇÃO:** empreitada por preço unitário - **FORMA DE PAGAMENTO**: Ordem Bancária.

PROCURADORIA GERAL DO ESTADO

RESUMO DE CONTRATO
Processo SEI nº. 006.7550.2022.0012628-16
Contrato nº PGE 015/2022 - Pregão Eletrônico 004/2022
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: **VTECH COMÉRCIO SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA**
Objeto: Renovação de licença/garantia das licenças de software antivírus utilizadas nas estações de trabalho e servidores da PGE, com garantia, contendo serviço de configuração/atualização e suporte on site. Valor Global estimado: R$ 162.940,00 (cento e sessenta e dois mil novecentos e quarenta reais). Unidade Orçamentária - 06.601, Fonte - 154, Projeto/Atividade - 7033, Elemento da Despesa - 33.90.40. Prazo: 12 (doze) meses, a contar da data de assinatura (11/04/2022). Regime de Execução/Forma de Pagamento: Empreitada por preço unitário.
Setor Responsável pela Gestão Contratual: Coordenação de Gestão Estratégica - CGE
Gestor: Eduardo Jorge Rodrigues Brandão
Fiscal: Mauricio de Cerqueira Pereira

RESUMO DE ADITIVO CONTRATUAL
Termo Aditivo 01 (Contrato PGE 015/2021)
Processo nº 006.7550.2021.0009826-01
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: EMPRESA GRÁFICA DA BAHIA - EGBA
Objeto: Prorrogar o contrato por 12 (doze) meses, com início em 14/04/2022 e término em 13/04/2023, cujas despesas serão atendidas pela Unidade Orçamentária - 06.601, Fonte - 300, Projeto/Atividade - 7033, Elemento de Despesa - 33.90.40, retificadas as cláusulas em desacordo com as modificações ora inseridas e ratificadas as demais.

SECRETARIA DA ADMINISTRAÇÃO

Departamento Estadual de Trânsito – DETRAN

RESUMO DO TERMO ADITIVO Nº 1º TERMO ADITIVO AO CONTRATO Nº 018/2021.
PROCESSO SEI Nº 049.4641.2022.0010024-95. **1.Contratante**: Departamento Estadual de Trânsito da Bahia - DETRAN/BA. **2. Contratada:** INTACTA PLANEJAMENTO E TRANSPORTE LTDA-ME, CNPJ sob o n.º 09.813.394/0001-71. **3. Objeto:** Acréscimo de 1.282,70 Km no quantitativo, representando aumento no percentual de 20,6747% do contrato, bem como a prorrogação da vigência do contrato por mais 60 (sessenta) dias. **4. Vigência:** com início em 12/04/2022 e término em 10/06/2022, para a execução do quantitativo de serviço acrescido. **5. Valor:** R$ 15.754,12 (quinze mil, setecentos e cinquenta e quatro reais e doze centavos). **6. Ordenador da Despesa:** Unidade Orçamentária: 09.301; Unidade Gestora: 0001; Ação: 06.122.315.2932.9900; Natureza da despesa: 33.90.39.00; Destinação de Recurso: 0.105.000000 e 0.213.00000. Assinatura: 11/04/2022 - Rodrigo Pimentel de Souza Lima - Diretor Geral.

SECRETARIA DE CULTURA

RESUMO DO TERMO ADITIVO Nº 03 AO CONTRATO
Nº 005/2019

PARTES: O ESTADO DA BAHIA / SECRETARIA DE CULTURA E A EMPRESA CALDAS SERVICE LTDA, OBJETO: EM DECORRÊNCIA DE JUSTIFICATIVAS APRESENTADAS NO PROCESSO ADMINISTRATIVO Nº 022.2249.2022.0000890-38 AS PARTES RESOLVEM ADITAR O CONTRATO ORIGINAL, PRORROGANDO POR MAIS 12 (DOZE) MESES, CONTADOS A PARTIR DE 10/05/2022 e com término em 09/05/2023. VALOR: R$ 800.393,28 (Oitocentos mil, trezentos e noventa e três reais e vinte e oito centavos). DOTAÇÃO: UNIDADE ORÇAMENTÁRIA: 3.22.101, FONTE: 100, PROJETO/ATIVIDADE: 13.122.502.2000, ELEMENTO DE DESPESA: 3.3.90.37 ASSINAM: ARANY SANTANA NEVES SANTOS E MELQUIZEDEQUE CORREIA CALDAS

SECRETARIA DE DESENVOLVIMENTO ECONÔMICO

Companhia Baiana de Pesquisa Mineral – CBPM

RESUMO DO II TERMO ADITIVO AO CONTRATO Nº 004/2020
PROCESSO SEI Nº 036.16106.2022.0000580-76 - **CONTRATANTE:** Companhia Baiana de Pesquisa Mineral - CBPM - **CONTRATADA:** DF Stamato & Cia Ltda. - **OBJETO**: Prorrogação do prazo de vigência do contrato - **DOTAÇÃO ORÇAMENTARIA:** Função: 22; Subfunção: 126; Programa: 502; Região de Planejamento: 9900; Ação: 2002 e Natureza da Despesa: 33.90.40.00 - **PRAZO:** 12 (doze) meses, entra em vigência no dia 11/07/2022 e expira em 10/07/2023 - **VALOR TOTAL ESTIMADO:** R$9.600,00 - **DATA DA ASSINATURA**: Salvador-Ba. 11/04/2022.