# EDITAL
# PREGÃO ELETRÔNICO Nº 12/2017-TCE/RN

O TRIBUNAL DE CONTAS DO ESTADO DO RIO GRANDE DO NORTE, localizado na Av. Getúlio Vargas, 690, Petrópolis, Natal/RN, por intermédio de sua Pregoeira, designada pela Portaria nº 005/2017-GP/TCE, de 17 de fevereiro de 2016, publicada no Diário Eletrônico do TCE/RN, edição de 18 de fevereiro de 2016, comunica aos interessados que realizará licitação na modalidade **PREGÃO**, na forma **ELETRÔNICA**, do tipo **MENOR PREÇO POR ITEM**, **às 9 (nove) horas do dia 03 de AGOSTO de 2017 (horário de Brasília)**, através do sítio www.comprasnet.gov.br, conforme Processo Administrativo nº 6933/2017-TC, nos termos da Lei n° 10.520, de 17 de julho de 2002, da Lei Complementar n° 123/06, da Resolução nº 007/2007-TCE/RN, de 19 de julho de 2007, da Resolução nº 009/2008-TCE/RN, de 17 de julho de 2008, das normas constantes da Lei nº 8.666, de 21 de junho de 1993, com as devidas alterações, de modo subsidiário, e pelas condições constantes neste Edital.

Observação: Ocorrendo decretação de feriado ou outro fato superveniente de caráter público, que impeça a realização do Pregão na data acima marcada, a licitação ficará automaticamente prorrogada para o primeiro dia útil subsequente, independentemente de nova comunicação.

## 1. DO OBJETO

1.1 - A presente licitação tem como objeto o Registro de Preços para eventual aquisição de 800 (oitocentas) licenças do software Kaspersky Endpoint Security for Business Advanced para estações de trabalho (desktops e laptops) e servidores, com criptografia de dados, segurança móvel, gerenciamento de dispositivos móveis e gerenciamento de sistemas, com atualizações para 36 meses, destinadas a atender às necessidades das Unidades Administrativas pertencentes ao TCE/RN, conforme especificações constantes no Anexo I deste Edital – Termo de Referência.

1.2 – Integram o presente Edital como se nele transcritos fossem:

Anexo I – Termo de Referência;
Anexo II – Minuta da Ata de Registro de Preços;
Anexo III – Minuta de Ordem de Serviço.
Anexo IV – Modelo de Declaração de Inexistência de Trabalhador Menor (inciso XXXIII do Art. 7º da Constituição Federal);
Anexo V – Modelo da Proposta;

## 2. DAS DISPOSIÇÕES PRELIMINARES

2.1 – O Pregão Eletrônico será realizado por meio de sistema eletrônico, mediante condições de segurança, utilizando-se de recursos de criptografia e de autenticação que viabilizem condições adequadas de segurança em todas as etapas do certame.

2.2 – Os trabalhos serão conduzidos pela Pregoeira, mediante a inserção e monitoramento de dados gerados ou transferidos para o aplicativo constante da página eletrônica do COMPRASNET, no endereço, www.comprasnet.gov.br.

2.3 – A solicitação de esclarecimento a respeito de condições deste Edital e de outros assuntos relacionados à presente licitação deverá ser efetuada através do site do COMPRASNET, no *email* pregaotce@gmail.com ou pelo telefone (084) 3642-7336, no prazo de até 2 (dois) dias úteis que anteceder a data estabelecida no preâmbulo deste instrumento convocatório para a sessão de recebimento das propostas de preços, conforme o art. 16 da Res. n.º 009/2008-TCE.

2.4 – A resposta da Pregoeira ao pedido de esclarecimento formulado será divulgada mediante publicação de nota no COMPRASNET e no endereço eletrônico www.tce.rn.gov.br, opção "Licitações". Nestas condições, cabe aos interessados acessá-los para a obtenção das informações prestadas.

2.5 – Todas as referências de tempo neste Edital observarão o horário de Brasília/DF.

2.6 – A licitante deverá observar, rigorosamente, as datas e o horário limite para o recebimento e a abertura das propostas, bem como para o início da disputa.

## 3. DAS CONDIÇÕES PARA PARTICIPAÇÃO

3.1 – Poderão participar deste Pregão Eletrônico as empresas que atendam às condições deste Edital e seus anexos, inclusive quanto à documentação, e estejam devidamente credenciadas perante o Comprasnet, para acesso ao sistema eletrônico.

3.2 - Para ter acesso ao sistema eletrônico, os interessados em participar deste Pregão deverão dispor de chave de identificação e senha pessoal, obtidas junto ao provedor do sistema, onde também deverão se informar a respeito do seu funcionamento e regulamento e receber instruções detalhadas para sua correta utilização.

3.3 - O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação por ela efetuada diretamente, ou por seu representante, não cabendo ao provedor do sistema ou ao TCE/RN responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

3.4 - Não poderão participar deste Pregão:

**a)** consórcio de empresa, que não atendam os requisitos disciplinados pelos art. 33 da Lei nº 8.666/93, art. 17 do Decreto nº 3.555/00 e o art. 16 do Decreto nº 5.450/05.

**b)** empresa suspensa de licitar e impedida de contratar com a Administração Pública, bem como os elencados na Lei nº 8.666/1993, art. 9º.

**c)** empresa que esteja declarada inidônea para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade;

**d)** empresa cujo objeto social não seja pertinente e compatível com o objeto deste Pregão;

**e)** empresas com falência, recuperação judicial, concordata ou insolvência, judicialmente decretadas, ou em processo de recuperação extrajudicial;

**f)** empresas em dissolução ou em liquidação.

3.5 - Como requisito para participação neste Pregão, a licitante deverá declarar, em campo próprio do sistema eletrônico, que está ciente e concorda com as condições contidas no Edital e seus Anexos e que cumpre plenamente os requisitos de habilitação definidos neste Edital.

3.6 - A declaração falsa relativa ao cumprimento dos requisitos de habilitação e à proposta sujeitará a licitante às sanções previstas neste Edital.

## 4. DO CREDENCIAMENTO

4.1 - O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico no site: www.comprasnet.gov.br.

4.2 - O credenciamento junto ao provedor do sistema implica responsabilidade legal da licitante ou de seu representante legal e presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

4.3 - O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao TCE/RN responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

## 5. DA PROPOSTA

5.1 – A licitante deverá, na forma expressa no sistema eletrônico, consignar os valores unitário e total, em moeda corrente nacional (R$), e a especificação do objeto ofertado, observado o disposto na Resolução 007/2007-TCE, art. 6°, III.

5.2 – Nos preços ofertados deverão já estar consideradas e inclusas todas as despesas incidentes sobre o objeto licitado, tais como: impostos, fretes, encargos e outras despesas incidentes sobre o fornecimento do objeto.

5.3 – Qualquer elemento que possa identificar a licitante importa a desclassificação da proposta.

5.4 – A simples participação no certame implica aceitação de todas as condições estabelecidas no Pregão, em especial:

a) que a proposta deverá ser mantida durante toda a vigência da Ata de Registro de Preços;
b) compromisso da licitante de entregar o(s) item(ns) cotado(s) na sede do Tribunal de Contas do Estado do Rio Grande do Norte - TCE/RN, pelo valor resultante de sua proposta ou do lance que a tenha consagrado vencedora, conforme o caso e nos termos do Anexo I deste Edital;
e) prazo para entrega de **30 (trinta) dias corridos**, contados a partir da data de recebimento da Ordem de Serviço/Nota de Empenho por parte do licitante vencedor;
f) Caso a proposta seja omissa, considerar-se-á que as suas especificações serão as que constam do Anexo I deste Edital.

5.5 – Os preços apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade da licitante, não lhe cabendo, neste caso, o direito de pleitear qualquer alteração.

**5.6 – Não será aceita a proposta que contenha preço com valores unitários acima daqueles encontrados na média da Pesquisa de preço constante no processo, salvo se houver justificativa expressa devidamente aceita pela Pregoeira, mediante consulta ao Setor Demandante.**

5.7 – Os quantitativos a serem cotados são aqueles constantes no Termo de Referência e no modelo de proposta.

## 6. DO ENVIO DA PROPOSTA ELETRÔNICA DE PREÇOS

6.1 – A licitante deverá encaminhar proposta exclusivamente por meio do sistema eletrônico, até a data e horário marcados para abertura da sessão, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas.

6.2 – Até a data e hora estabelecidos para a abertura da sessão, a licitante poderá retirar ou substituir a proposta anteriormente encaminhada.

## 7. DA ABERTURA DA SESSÃO PÚBLICA

7.1 – A abertura da sessão pública deste Pregão, conduzida pela Pregoeira, ocorrerá na data e na hora indicadas no preâmbulo deste Edital, no site www.comprasnet.gov.br.

7.2 – A comunicação entre a Pregoeira e as licitantes ocorrerá exclusivamente mediante mensagens em campo próprio do sistema eletrônico.

7.3 – Cabe à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

## 8. DA CLASSIFICAÇÃO DAS PROPOSTAS

8.1 – A pregoeira verificará as propostas apresentadas e desclassificará, motivadamente, aquelas que não estiverem em conformidade com os requisitos estabelecidos neste Edital.

8.2 – Serão desclassificadas as propostas de preços que:

a) não atenderem às exigências deste Edital;
b) apresentarem, após a fase de lances ou negociação, valores superiores à média de preços da pesquisa de mercado.

8.3 – A desclassificação de proposta será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

8.4 – Somente as licitantes com propostas classificadas participarão da fase de lances.

8.5 – Os erros, equívocos e omissões havidos nas cotações serão de inteira responsabilidade do proponente, não lhe cabendo, em caso de classificação, eximir-se do fornecimento do objeto da presente licitação.

## 9. DA FORMULAÇÃO DE LANCES E DA ACEITABILIDADE DA PROPOSTA

9.1 – A etapa competitiva será aberta na data e na hora indicada no primeiro parágrafo deste edital, a partir da qual as licitantes classificadas poderão encaminhar lances, exclusivamente por meio do sistema eletrônico, sendo imediatamente informadas do recebimento e respectivo horário de registro e valor.

9.2 – As licitantes poderão oferecer lances sucessivos, não sendo aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar pelo sistema.

9.3 – A licitante somente poderá oferecer lance inferior ao último por ela ofertado e registrado no sistema.

9.4 – Durante o transcurso da sessão, as licitantes serão informadas, em tempo real, do valor do menor lance registrado, vedada a identificação da ofertante.

9.5 – Os lances apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade da licitante, não lhe cabendo o direito de pleitear qualquer alteração.

9.6 – Durante a fase de lances, a Pregoeira poderá excluir, justificadamente, lance cujo valor for considerado inexequível.

9.7 – A etapa de lances da sessão pública será encerrada por decisão da Pregoeira mediante aviso de fechamento iminente.

9.8 – O sistema eletrônico encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado pelo sistema, findo o qual será automaticamente encerrada a recepção de lances.

9.9 – Se ocorrer a desconexão da Pregoeira no decorrer da etapa de lances e o sistema eletrônico permanecer acessível às licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

9.10 – No caso da desconexão da Pregoeira persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão será suspensa automaticamente e terá reinício somente após comunicação expressa aos participantes no sítio www.comprasnet.gov.br.

9.11 – Após o encerramento da etapa de lances, a Pregoeira poderá encaminhar contraproposta diretamente à licitante que tenha apresentado o lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento e o valor estimado para a contratação, não se admitindo negociar condições diferentes das previstas neste Edital.

9.12 – A negociação será realizada por meio do sistema, podendo ser acompanhada pelas demais licitantes.

9.13 – Encerrada a etapa de lances e concluída a negociação, quando houver, a Pregoeira examinará a proposta classificada em primeiro lugar quanto à compatibilidade do preço em relação ao valor estimado para a contratação, consoante média de preços da pesquisa mercadológica.

9.13.1 - Não será aceita a proposta que contenha preço unitário com valor acima daquele encontrado na média da Pesquisa de Preço constante no processo, salvo se houver justificativa expressa devidamente aceita pela Pregoeira, mediante consulta ao Setor Demandante.

9.14 – Não se considerará qualquer oferta de vantagem não prevista neste Edital.

9.15 – Será rejeitada a proposta que apresentar valores irrisórios ou de valor zero, incompatíveis com os preços de mercado acrescidos dos respectivos encargos.

9.16 – A Pregoeira poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do TCE/RN ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para verificar a aceitabilidade das propostas caso tenha alguma dúvida.

9.17 – Havendo aceitação da proposta classificada em primeiro lugar quanto à compatibilidade de preço, a Pregoeira solicitará da respectiva licitante o encaminhamento dos documentos de habilitação.

9.18 – Se a proposta não for aceitável ou se a licitante não atender às exigências habilitatórias, a Pregoeira examinará a proposta subsequente e, assim, sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda a este Edital.

9.19 – A Pregoeira poderá solicitar documentos que comprovem o enquadramento da licitante na categoria de microempresa ou empresa de pequeno porte.

9.20 – Quanto à parte do objeto não exclusiva para ME/EPP, após a fase de lances e da negociação, se a proposta mais bem classificada não tiver sido ofertada por microempresa ou empresa de pequeno porte e houver proposta apresentada por microempresa ou empresa de pequeno porte igual ou até 5% (cinco por cento) superior à melhor proposta, proceder-se-á da seguinte forma:

a) a microempresa ou empresa de pequeno porte mais bem classificada poderá, no prazo de 5 (cinco) minutos após a convocação, apresentar nova proposta inferior àquela considerada vencedora do certame, situação em que será adjudicado em seu favor o objeto deste Pregão;
b) não ocorrendo a contratação da microempresa ou empresa de pequeno porte, na forma do subitem anterior, serão convocadas as licitantes remanescentes que porventura se enquadrem na hipótese desta Condição, na ordem classificatória, para o exercício do mesmo direito;
c) no caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nesta Condição, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta;
d) a microempresa ou empresa de pequeno porte mais bem classificada será convocada para apresentar nova proposta no prazo máximo de 5 (cinco) minutos após a solicitação da Pregoeira, sob pena de preclusão;
e) a Pregoeira poderá solicitar documentos que comprovem o enquadramento da licitante na categoria de microempresa ou empresa de pequeno porte.

9.21 – Na hipótese da não-contratação nos termos previstos na condição anterior, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame.

## 10. DAS AMOSTRAS

10.1 - O Tribunal de Contas reserva-se o direito de solicitar amostra do produto para análise e o licitante vencedor se obriga a encaminhá-la no prazo máximo de 05 (cinco) dias úteis contados a partir da notificação encaminhada pela pregoeira;

10.2 - O prazo estabelecido no item anterior para apresentação da amostra é improrrogável, portanto, não serão aceitos quaisquer pedidos de prorrogação do mesmo, salvo a comprovação do envio do produto por empresa transportadora ou Correio.

10.3 - As amostras dos itens licitados serão analisadas pelo setor competente, utilizando-se por base os critérios objetivamente definidos no termo de referência para aceitação do objeto, o qual emitirá o Relatório de Análise de Material, informando a aceitação ou recusa dos mesmos, resguardado o direito dos concorrentes de acompanharem todos os procedimentos respectivos, em data e hora informada pela Pregoeira para a divulgação do resultado;

10.3.1 - O prazo para análise e apresentação do resultado das amostras será informado pela Pregoeira no momento da solicitação das amostras.

10.4 - As amostras aprovadas permanecerão em poder da Administração, sob sua guarda e responsabilidade, até a primeira compra realizada por este Órgão ao licitante vencedor.

10.5 - As amostras recusadas deverão ser retiradas pelo licitante no prazo máximo de 5 (cinco) dias úteis, no prédio Sede do Tribunal de Contas, após recebimento de notificação.

10.6 - As amostras que não forem retiradas dentro do prazo estabelecido serão destruídas.

## 11. DA HABILITAÇÃO

11.1 – Para fins de habilitação no presente certame se faz necessária a apresentação dos seguintes documentos:

### 11.1.1 – HABILITAÇÃO JURÍDICA:

a) registro comercial, no caso de empresa individual (Requerimento de Empresário);
b) ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores. No caso de alterações, será admitido o estatuto ou o contrato social consolidado e aditivos posteriores (se houver);
c) inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;
d) decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

**11.1.2 – QUALIFICAÇÃO TÉCNICA:**

a) atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, que comprove(m) que a empresa prestou ou está prestando, a contento, o fornecimento de objeto em características compatíveis ao deste Pregão.

**11.1.3 – QUALIFICAÇÃO ECONÔMICA-FINANCEIRA:**

**a)** Certidão Negativa de Falência ou Recuperação Judicial expedida pelo Distribuidor da sede da Licitante.
**b)** Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;
b.1) no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;
**c)** Comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), resultantes da aplicação das fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

**d)** As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido não inferior a 10% do valor estimado da contratação ou do item pertinente.

**11.1.4 – REGULARIDADE FISCAL**

a) Comprovante de Inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ, expedido pela Receita Federal;
b) Certidão de Regularidade do FGTS - CRF, emitido pela Caixa Econômica Federal;
c) Certidão Conjunta Negativa (ou positiva com efeito de negativa) de Débitos relativos aos Tributos Federais e à Dívida Ativa da União, emitida pela Procuradoria Geral da Fazenda Nacional em conjunto com a Receita Federal do Brasil;
d) Certidão Negativa (ou positiva com efeito de negativa) de Débito do Estado do domicílio ou sede do licitante;

**11.1.5 – DECLARAÇÃO DO MENOR:**

a) Declaração da licitante de que não possui em seu quadro de pessoal empregado(s) com menos de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, nos termos do inciso XXXIII do art. 7º da Constituição Federal.

**11.1.6 – CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS:**

a) Certidão Negativa de Débitos Trabalhistas, emitida pelo Tribunal Superior do Trabalho, nos termos da Lei nº 12.440, de 07 de julho de 2011.

11.2 – Sob pena de inabilitação, todos os documentos apresentados para habilitação deverão estar em nome da licitante e, preferencialmente, com número do CNPJ e endereço respectivo, observando-se que:

a) se a licitante for a matriz, todos os documentos deverão estar em nome da matriz; ou
b) se a licitante for a filial, todos os documentos deverão estar em nome da filial;
c) serão dispensados da filial aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

11.3 – A proposta ajustada ao lance final da licitante vencedora e os documentos exigidos para habilitação, inclusive quando houver necessidade de envio de anexos, deverão ser remetidos via fac-símile, para o número (84) 3642-7336, ou para o endereço eletrônico pregaotce@rn.gov.br e pregaotce@gmail.com, no prazo de 60 (sessenta) minutos, contados da solicitação da Pregoeira. Este prazo pode ser prorrogado pela Pregoeira de acordo com a necessidade e mediante justificativa.

11.4 – A proposta final, os documentos para habilitação e os anexos remetidos via fac-símile ou por meio eletrônico deverão ser encaminhados em original ou por cópia autenticada, no prazo de 3 (três) dias úteis, contados da solicitação da Pregoeira, ao Setor de Licitações, na sede do Tribunal, 2º andar.

11.5 – Os modelos anexados a este Edital servem apenas como orientação, não sendo motivo de impedimento ou desclassificação, a apresentação de declarações que sejam elaboradas de forma diferente e que contenham os elementos essenciais.

11.6 – As empresas que integram o Sistema de Cadastramento Unificado de Fornecedores – SICAF ficam desobrigadas de apresentarem os documentos exigidos nos itens 11.1.1 e 11.1.4 desta cláusula, cuja verificação far-se-á através de consulta on-line ao referido sistema.

11.6.1 – Após a consulta no SICAF, será impresso pela Pregoeira e integrará a documentação de habilitação dos licitantes o(s) documento(s) referente(s) à "situação do fornecedor".

11.7 – Será inabilitada a licitante que apresentar na consulta ao SICAF documento fora do prazo de validade, salvo se sanada a situação na sessão pública de processamento deste Pregão, por meio da apresentação via fax, no prazo estabelecido no item 11.3, dos documentos por parte da licitante e/ou verificação efetuada por meio eletrônico hábil de informações (internet), oportunidade também, que será concedida às demais licitantes não cadastradas.

11.8 – A verificação de que trata o item anterior será de forma imediata, na própria sessão, certificada pela Pregoeira e os respectivos documentos anexados aos autos, salvo impossibilidade de verificação devidamente justificada.

11.9 – O TCE/RN não se responsabilizará pela eventual indisponibilidade dos meios eletrônicos, no momento da verificação da habilitação. Ocorrendo essa indisponibilidade e não sendo apresentados os documentos alcançados pela verificação, a licitante será inabilitada.

11.10 – As licitantes que deixarem de apresentar quaisquer dos documentos exigidos para habilitação na presente licitação, ou os apresentarem em desacordo com o estabelecido neste edital ou com irregularidades serão inabilitadas, salvo se sanada a situação, conforme previsto no item 11.7.

11.11 – Os documentos exigidos e apresentados para habilitação, obtidos através de sites, poderão ter sua autenticidade verificada via internet, no momento da fase de habilitação.

11.12 – Havendo alguma restrição na comprovação da regularidade fiscal, as microempresas e empresas de pequeno porte terão prazo adicional de 5 (cinco) dias úteis, contado da decisão da Pregoeira que declarar a empresa vencedora do certame, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa, prorrogável por igual período à critério da administração.

11.13 – A não regularização da documentação, no prazo previsto no item anterior, implicará na inabilitação da licitante, sem prejuízo das sanções previstas neste Edital, sendo facultado ao TCE/RN convocar as licitantes remanescentes, na ordem de classificação, para a assinatura do contrato, ou propor a revogação deste Pregão.

## 12. DA IMPUGNAÇÃO DO EDITAL E DO RECURSO

12.1 – Até 2 (dois) dias úteis antes da data fixada para recebimento das propostas, qualquer pessoa poderá impugnar o ato convocatório do pregão. Caberá à Pregoeira decidir sobre a petição no prazo de até 24 (vinte e quatro) horas. Acolhida a petição contra o ato convocatório, será designada nova data para a realização do certame.

12.2 – Declarado o vencedor, a Pregoeira abrirá prazo de 30 (trinta) minutos, durante o qual qualquer licitante poderá, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recorrer.

12.3 – A Pregoeira fará juízo de admissibilidade da intenção de recorrer manifestada, aceitando-a ou, motivadamente, rejeitando-a, em campo próprio do sistema, bem como fará o recebimento, o exame e a decisão dos recursos, conforme previsto na Resolução nº 009/2008-TCE, art. 12, inc. VIII, remetendo - o, de ofício, à Autoridade Competente para decisão final.

12.3.1 – Os recursos serão decididos de acordo com o regramento constante da referida Resolução.

12.4 – A recorrente que tiver sua intenção de recurso aceita deverá registrar as razões do recurso, em campo próprio do sistema, no prazo de 3 (três) dias, ficando as demais licitantes, desde logo, intimadas a apresentar contrarrazões, também via sistema, em igual prazo, que começará a correr do término do prazo da recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

12.5 – A falta de manifestação imediata e motivada da intenção de interpor recurso, no momento da sessão pública deste Pregão, implica decadência desse direito, ficando a Pregoeira autorizado a adjudicar o objeto à licitante vencedora.

12.6 – O acolhimento do recurso importará invalidação apenas dos atos insuscetíveis de aproveitamento.

12.7 – Qualquer recurso contra a decisão da Pregoeira terá, em regra, efeito suspensivo.

## 13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1 – A Pregoeira, caso não haja recurso ao julgamento do certame, adjudicará o objeto à licitante vencedora cuja proposta for considerada mais vantajosa à administração pública.

13.2 – Concluídos os trabalhos, a Pregoeira encaminhará o processo, devidamente instruído, à apreciação da Excelentíssima Senhor Secretário Geral do Tribunal de Contas do Estado do Rio Grande do Norte, para expedição e publicação do ato homologatório.

13.3 – Após decididos os recursos, quando houver, e constatada a regularidade dos atos procedimentais, o Secretário Geral adjudicará o objeto ao vencedor do certame e, em consequência, homologará a presente licitação.

## 14. DOS PROCEDIMENTOS PARA O REGISTRO DE PREÇOS

14.1 – Homologado o resultado da licitação, a Comissão de Gerenciamento do Sistema de Registro de Preços do TCE/RN formalizará a Ata de Registro de Preços com o fornecedor primeiro classificado e, se for o caso, com os demais classificados, obedecida a ordem de classificação e os quantitativos propostos.

14.2 – O Setor Gerenciador do TCE/RN convocará o fornecedor a ser registrado, que terá prazo de até 05 (cinco) dias úteis, contados da convocação, salvo motivo justificado e devidamente aceito, para a assinatura da Ata de Registro de Preços.

14.3 – Como condição para assinatura da Ata de Registro de Preços, bem como para as aquisições dela resultantes, a licitante vencedora deverá manter todas as condições de Habilitação, de acordo com o inciso XIII do art. 55 da Lei nº 8.666/93 (Estatuto de Licitações e Contratos).

14.4 – No caso do fornecedor primeiro classificado, depois de convocado, não comparecer ou se recusar a assinar a Ata de Registro de Preços, sem prejuízo das punições previstas neste Edital, serão registrados os demais licitantes, mantido a ordem de classificação.

14.5 – A partir da publicação da Ata de Registro de Preços no Diário Eletrônico Tribunal de Contas do Estado do Rio Grande do Norte, a licitante se obriga a cumprir, na sua íntegra, todas as condições estabelecidas, ficando sujeita às penalidades pelo descumprimento de quaisquer de suas cláusulas.

14.6 – A Ata de Registro de Preços terá validade de 12 (doze) meses, contada da assinatura.

14.7 – A existência de preços registrados não obriga o TCE/RN a firmar as contratações que deles poderão advir, facultando-se a realização de licitação específica para a aquisição pretendida, sendo assegurado ao beneficiário do registro preferência de fornecimento em igualdade de condições.

14.8 – Comprovada a redução dos preços praticados no mercado nas mesmas condições do registro, e, definido o novo preço máximo a ser pago pelo TCE/RN, o fornecedor registrado será convocado pela Comissão de Gerenciamento do Sistema de Registro de Preços do TCE/RN para a devida alteração do valor registrado na Ata de Registro de Preços.

14.9 – O Fornecedor terá seu registro cancelado quando:

a) não cumprir as exigências do instrumento convocatório que deu origem ao registro de preços;
b) não assinar o Ata de Registro de Preços decorrente ou não retirar, no prazo estabelecido pelo Tribunal, o instrumento equivalente, dentre os previstos no art. 62 da Lei nº 8.666/93, salvo se aceita sua justificativa;
c) não aceitar reduzir o preço registrado, na hipótese de este se tornar superior àqueles praticados no mercado;
d) der causa a rescisão administrativa de contrato decorrente do registro de preços;
e) ocorrer qualquer das hipóteses de inexecução total ou parcial de contrato, relativamente a contratação decorrente do registro de preços por ele formalizada;
f) tiver presentes razões de interesse público, devidamente fundamentadas, ou houver hipótese prevista em lei; e
g) mediante solicitação sua, por escrito, quando comprovar a impossibilidade de cumprimento da perfeita execução contratual, decorrente de caso fortuito ou de força maior.

14.10 – O cancelamento de registro nas hipóteses previstas nas alíneas "a" a "f" do item anterior, assegurado o contraditório e a ampla defesa, será formalizado por despacho da autoridade competente da Diretoria de Administração Geral do TCE/RN.

14.11 – A Ata de Registro de Preços será cancelada automaticamente:

a) por decurso de prazo de vigência;
b) quando não restarem fornecedores registrados.

## 15. DO CONTRATO

15.1 – Conforme preceitua o art. 62, parágrafo 4º da Lei Complementar nº 8.666/93, o termo de contrato será substituído pela a Ordem de Serviço.

## 16. DO PRAZO

16.1 – O objeto desta licitação deverá ser entregue no prazo máximo de 30 (trinta) dias corridos, contados do recebimento da respectiva Ordem de Serviço/Nota de Empenho.

## 17. DO PAGAMENTO

17.1– Conforme preceitua o item 6 da Ata de Registro de Preços.

## 18. DAS SANÇÕES ADMINISTRATIVAS

18.1 – As sanções administrativas estão elencadas no item 9 da Ata de Registro de Preços.

## 19. DAS DISPOSIÇÕES FINAIS

19.1 – O Secretário Geral do TCE/RN, na defesa do interesse do serviço público e de acordo com a legislação vigente, reserva-se ao direito de anular ou revogar, no todo ou em parte, a presente licitação.

19.2 – Decairá do direito de impugnar os termos deste Edital, apontando as falhas ou irregularidades que o viciarem, a licitante que não o fizer até o segundo dia útil que anteceder a entrega da proposta, hipótese em que tal comunicação não terá efeito de recurso.

19.3 – A participação nesta licitação implica aceitação plena e irrevogável das normas constantes do presente ato de convocação, independentemente de declaração expressa.

19.4 – Na contagem dos prazos deste Edital, será excluído o dia de início e incluído o dia do vencimento, considerando-se o expediente normal desta Corte de Contas, o qual compreende o horário das 8 às 18 horas, de segunda à quinta-feira, e das 7 às 13 horas, na sexta-feira.

19.5 – A Pregoeira, no interesse da Administração, poderá relevar omissões puramente formais observadas na documentação e na proposta de preço, desde que não contrariem a legislação vigente e não comprometam a lisura da licitação, sendo possível a promoção de diligência destinada a esclarecer ou a convalidar a instrução do processo.

19.6 – Os casos omissos serão dirimidos pela Pregoeira, com observância da legislação vigente, em especial a Lei n° 10.520, de 17 de julho de 2002, a Lei Complementar n° 123/2006, a Resolução nº 007/2007-TCE/RN, de 19 de julho de 2007, a Resolução nº 009/2008-TCE/RN, de 17 de julho de 2008, e, subsidiariamente, as normas constantes da Lei nº 8.666, de 21 de junho de 1993, com as devidas alterações.

Natal (RN), 22 de junho de 2017.

**VANESSA DE SOUSA MENEZES UBARANA**
Pregoeira do TCE/RN

**PREGÃO ELETRÔNICO N° 012/2017 – TCE/RN**
**ANEXO I – TERMO DE REFERÊNCIA**

## 1. OBJETIVO

A formação de Ata de Registro de Preços (ARP) para posterior aquisição de 800 (oitocentas) licenças do software Kaspersky Endpoint Security for Business Advanced para estações de trabalho (desktops e laptops) e servidores, com criptografia de dados, segurança móvel, gerenciamento de dispositivos móveis e gerenciamento de sistemas, com atualizações para 36 meses, destinadas a atender às necessidades das Unidades Administrativas pertencentes ao TCE/RN.

## 2. JUSTIFICATIVA DA AQUISIÇÃO

Proteger o sigilo, a integridade e a disponibilidade das informações por meio da prevenção contra a contaminação por vírus, malwares e suas variantes nos computadores da instituição. Estas aquisições diminuirão possíveis transtornos na área de segurança, possibilitando um maior desempenho das estações de trabalho e, por conseguinte, uma melhor condição aos técnicos na realização de suas atividades.

## 3. PRODUTO E ESPECIFICAÇÃO TÉCNICA

Os produtos, objeto da composição do registro de preços em referência, correspondem aos itens discriminados e devidamente especificados, conforme se segue:

### 3.1.Servidor de Administração e Console Administrativa:

3.1.1.Compatibilidade:

3.1.1.1.Microsoft Windows Server 2003 SP2 (Todas edições);

3.1.1.2. Microsoft Windows Server 2003 x64 SP2 (Todas edições);

3.1.1.3. Microsoft Windows Server 2008 (Todas edições);

3.1.1.4.Microsoft Windows Server 2008 x64 SP1 (Todas edições);

3.1.1.5.Microsoft Windows Server 2008 R2 (Todas edições);

3.1.1.6.Microsoft Windows Server 2012 (Todas edições);

3.1.1.7.Microsoft Windows Server 2012 R2 (Todas edições);

3.1.1.8.Microsoft Windows Small Business Server 2003 SP2 (Todas edições);

3.1.1.9.Microsoft Windows Small Business Server 2008 (Todas edições);

3.1.1.10.Microsoft Windows Small Business Server 2011 (Todas edições);

3.1.1.11.Microsoft Windows XP Professional SP2 ou superior;

3.1.1.12. Microsoft Windows XP Professional x64 SP2 ou superior;

3.1.1.13.Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;

3.1.1.14.Microsoft Windows Vista Business / Enterprise / Ultimate SP1 x64 ou posterior;

3.1.1.15.Microsoft Windows 7 Professional / Enterprise / Ultimate;

3.1.1.16.Microsoft Windows 7 Professional / Enterprise / Ultimate x64;

3.1.1.17.Microsoft Windows 8 Professional / Enterprise;

3.1.1.18.Microsoft Windows 8 Professional / Enterprise x64;

3.1.1.19.Microsoft Windows 8.1 Professional / Enterprise;

3.1.1.20.Microsoft Windows 8.1 Professional / Enterprise x64.

3.1.2.Características:

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

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

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

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

3.1.7. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;

3.1.8.As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o

produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

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

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

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

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

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

3.1.14. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;

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

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

3.1.17. 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;

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

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

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

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

3.1.22. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

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

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

3.1.25.Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

3.1.25.1.1.Nome do computador;

3.1.25.1.2.Nome do domínio;

3.1.25.1.3.Range de IP;

3.1.25.1.4.Sistema Operacional;

3.1.25.1.5.Máquina virtual.

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

3.1.27.Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

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

3.1.29.Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

3.1.30.Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

3.1.31.Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

3.1.32.Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

3.1.33.Deve fornecer as seguintes informações dos computadores:

3.1.33.1.Se o antivírus está instalado;

3.1.33.2.Se o antivírus está iniciado;

3.1.33.3.Se o antivírus está atualizado;

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

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

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

3.1.33.7.Versão do antivírus instalado na máquina;

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

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

3.1.33.10.Quantidade de vírus encontrados (contador) na máquina;

3.1.33.11.Nome do computador;

3.1.33.12.Domínio ou grupo de trabalho do computador;

3.1.33.13.Data e horário da última atualização de vacinas;

3.1.33.14.Sistema operacional com Service Pack;

3.1.33.15.Quantidade de processadores;

3.1.33.16.Quantidade de memória RAM;

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

3.1.33.18.Endereço IP;

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

3.1.33.20.Atualizações do Windows Updates instaladas;

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

3.1.33.22.Vulnerabilidades de aplicativos instalados na máquina;

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

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

3.1.35.1.Alteração de Gateway Padrão;

3.1.35.2.Alteração de subrede;

3.1.35.3.Alteração de domínio;

3.1.35.4.Alteração de servidor DHCP;

3.1.35.5.Alteração de servidor DNS;

3.1.35.6.Alteração de servidor WINS;

3.1.35.7.Alteração de subrede;

3.1.35.8.Resolução de Nome;

3.1.35.9.Disponibilidade de endereço de conexão SSL;

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

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

3.1.38.Capacidade de relacionar servidores em estrutura de hierarquia para obter

relatórios sobre toda a estrutura de antivírus;

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

3.1.40.Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

3.1.41.Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

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

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

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

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

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

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

3.1.48.Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

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

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

3.1.51.Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

3.1.51.1.Nome do vírus;

3.1.51.2.Nome do arquivo infectado;

3.1.51.3.Data e hora da detecção;

3.1.51.4.Nome da máquina ou endereço IP;

3.1.51.5.Ação realizada.

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

3.1.53.Capacidade de realizar inventário de hardware de todas as máquinas clientes;

3.1.54.Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

3.1.55.Capacidade de diferenciar máquinas virtuais de máquinas físicas.

**3.2.Estações Windows**

3.2.1.Compatibilidade:

3.2.1.1. Microsoft Windows Embedded 8.0 Standard x64;

3.2.1.2.Microsoft Windows Embedded 8.1 Industry Pro x64;

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

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

3.2.1.5.Microsoft Windows XP Professional x86 SP3 e superior;

3.2.1.6. Microsoft Windows Vista x86 / x64SP2 e posterior;

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

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

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

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

3.2.2.Características:

3.2.2.1. Deve prover as seguintes proteções:

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

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

3.2.2.1.3.Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

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

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

3.2.2.1.6.Firewall com IDS;

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

3.2.2.1.8.Controle de dispositivos externos;

3.2.2.1.9.Controle de acesso a sites por categoria;

3.2.2.1.10.Controle de acesso a sites por horário;

3.2.2.1.11.Controle de acesso a sites por usuários;

3.2.2.1.12.Controle de execução de aplicativos;

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

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

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

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

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

3.2.2.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

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

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

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

3.2.2.10.Capacidade de verificar somente arquivos novos e alterados;

3.2.2.11.Capacidade de verificar objetos usando heurística;

3.2.2.12.Capacidade de agendar uma pausa na verificação;

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

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

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

3.2.2.15.1.Perguntar o que fazer, ou;

3.2.2.15.2.Bloquear acesso ao objeto;

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

3.2.2.15.2.2.Caso positivo de desinfecção:

3.2.2.15.2.2.1.Restaurar o objeto para uso;

3.2.2.15.2.3.Caso negativo de desinfecção:

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

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

3.2.2.17.Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);

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

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

3.2.2.20.Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;

3.2.2.21.Capacidade de verificação de corpo e anexos de e-mails usando heurística;

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

3.2.2.22.1.Perguntar o que fazer, ou;

3.2.2.22.2.Bloquear o e-mail;

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

3.2.2.22.2.2.Caso positivo de desinfecção:

3.2.2.22.2.2.1.Restaurar o e-mail para o usuário;

3.2.2.22.2.3.Caso negativo de desinfecção:

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

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

3.2.2.24.Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

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

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

3.2.2.27.Deve ter suporte total ao protocolo IPv6;

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

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

3.2.2.29.1.Perguntar o que fazer, ou;

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

3.2.2.29.3.Permitir acesso ao objeto;

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

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

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

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

3.2.2.32.Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

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

3.2.2.34.Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou

gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

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

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

3.2.2.37.Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;

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

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

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

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

3.2.2.39.1.Discos de armazenamento locais;

3.2.2.39.2.Armazenamento removível;

3.2.2.39.3.Impressoras;

3.2.2.39.4.CD/DVD;

3.2.2.39.5.Drives de disquete;

3.2.2.39.6.Modems;

3.2.2.39.7.Dispositivos de fita;

3.2.2.39.8.Dispositivos multifuncionais;

3.2.2.39.9.Leitores de smart card;

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

3.2.2.39.11.Wi-Fi;

3.2.2.39.12.Adaptadores de rede externos;

3.2.2.39.13.Dispositivos MP3 ou smartphones;

3.2.2.39.14.Dispositivos Bluetooth;

3.2.2.39.15.Câmeras e Scanners.

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

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

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

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

3.2.2.44.Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;

3.2.2.45.Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

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

3.2.2.47.Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

3.2.2.48.Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer

configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

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

**3.3.Estações Mac OS X**

3.3.1.Compatibilidade:

3.3.1.1.Mac OS X 10.11 (El Capitan);

3.3.1.2.Mac OS X 10.10 (Yosemite);

3.3.1.3.Mac OS X 10.9 (Mavericks).

3.3.1.4.Mac OS X 10.8 (Mountain Lion)

3.3.1.5.Mac OS X 10.7 (Lion)

3.3.2.Características:

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

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

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

3.3.2.4. Deve possuir suportes a notificações utilizando o Growl;

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

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

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

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

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

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

3.3.2.11.Capacidade de verificar somente arquivos novos e alterados;

3.3.2.12.Capacidade de verificar objetos usando heurística;

3.3.2.13.Capacidade de agendar uma pausa na verificação;

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

3.3.3.1.Perguntar o que fazer, ou;

3.3.3.2.Bloquear acesso ao objeto;

3.3.3.3.Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);Caso positivo de desinfecção:

3.3.3.4.Restaurar o objeto para uso;

3.3.4.Caso negativo de desinfecção:

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

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

3.3.4.2.Capacidade de verificar arquivos de formato de email;

3.3.4.3.Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

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

**3.4.Estações de trabalho Linux**

3.4.1.Compatibilidade:

3.4.1.1. Plataforma 32-bits:

3.4.1.1.1.Canaima 3;

3.4.1.1.2.Red Flag Desktop 6.0 SP2;

3.4.1.1.3.Red Hat Enterprise Linux 5.8 Desktop;

3.4.1.1.4.Red Hat Enterprise Linux 6.2 Desktop;

3.4.1.1.5.Fedora 16;

3.4.1.1.6.CentOS-6.2;

3.4.1.1.7.SUSE Linux Enterprise Desktop 10 SP4;

3.4.1.1.8.SUSE Linux Enterprise Desktop 11 SP2;

3.4.1.1.9.openSUSE Linux 12.1;

3.4.1.1.10.openSUSE Linux 12.2;

3.4.1.1.11.Debian GNU/Linux 6.0.5;

3.4.1.1.12.Mandriva Linux 2011;

3.4.1.1.13.Ubuntu 10.04 LTS;

3.4.1.1.14.Ubuntu 12.04 LTS.

3.4.1.1.15.

3.4.1.2.Plataforma 64-bits:

3.4.1.2.1.Canaima 3;

3.4.1.2.2.Red Flag Desktop 6.0 SP2;

3.4.1.2.3.Red Hat Enterprise Linux 5.8;

3.4.1.2.4.Red Hat Enterprise Linux 6.2 Desktop;

3.4.1.2.5.Fedora 16;

3.4.1.2.6.CentOS-6.2;

3.4.1.2.7.SUSE Linux Enterprise Desktop 10 SP4;

3.4.1.2.8.SUSE Linux Enterprise Desktop 11 SP2;

3.4.1.2.9.openSUSE Linux 12.1;

3.4.1.2.10.openSUSE Linux 12.2;

3.4.1.2.11.Debian GNU/Linux 6.0.5;

3.4.1.2.12.Ubuntu 10.04 LTS;

3.4.1.2.13.Ubuntu 12.04 LTS.

3.4.2.Características:

3.4.3. Deve prover as seguintes proteções:

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

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

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

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

3.4.4.2.Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

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

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

remoção de objetos infectados.

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

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

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

3.4.8. Capacidade de verificar objetos usando heurística;

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

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

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

**3.5.Servidores Windows**

3.5.1.Compatibilidade:

3.5.2.Plataforma 32-bits:

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

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

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

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

3.5.2.5.Plataforma 64-bits:

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

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

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

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

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

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

3.5.2.5.7.Microsoft Windows Storage Server 2008 R2;

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

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

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

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

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

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

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

3.5.2.5.15.Microsoft Windows Hyper-V Server 2012;

3.5.2.5.16.Microsoft Windows Hyper-V Server 2012 R2.

3.5.2.6.Características:

3.5.2.6.1. Deve prover as seguintes proteções:

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

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

3.5.2.6.1.3.Firewall com IDS;

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

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

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

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

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

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

3.5.2.6.4.3.Leitura de configurações;

3.5.2.6.4.4.Modificação de configurações;

3.5.2.6.4.5.Gerenciamento de Backup e Quarentena;

3.5.2.6.4.6.Visualização de relatórios;

3.5.2.6.4.7.Gerenciamento de relatórios;

3.5.2.6.4.8.Gerenciamento de chaves de licença;

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

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

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

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

3.5.2.6.6.Capacidade de separadamente selecionar o número de processos que irão executar

funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

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

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

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

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

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

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

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

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

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

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

3.5.2.6.17.Capacidade de verificar somente arquivos novos e alterados;

3.5.2.6.18.Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos

comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

3.5.2.6.19.Capacidade de verificar objetos usando heurística;

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

3.5.2.6.21.Capacidade de agendar uma pausa na verificação;

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

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

3.5.2.6.23.1.Perguntar o que fazer, ou;

3.5.2.6.23.2.Bloquear acesso ao objeto;

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

3.5.2.6.23.2.2.Caso positivo de desinfecção:

3.5.2.6.23.2.2.1.Restaurar o objeto para uso;

3.5.2.6.23.2.3.Caso negativo de desinfecção:

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

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

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

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

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

**3.6.Servidores Linux**

3.6.1.Compatibilidade:

3.6.2. Plataforma 32-bits:

3.6.2.1.Red Hat Enterprise Linux Server 5.x;

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

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

3.6.2.4.SUSE® Linux Enterprise Server 11 SP3;

3.6.2.5.Ubuntu Server 12.04 LTS;

3.6.2.6.Ubuntu Server 14.04 LTS;

3.6.2.7.Ubuntu Server 14.10;

3.6.2.8.Oracle Linux 6.5;

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

3.6.2.10.openSUSE 13.1.

3.6.3.Plataforma 64-bits:

3.6.3.1.Red Hat Enterprise Linux Server 5.x;

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

3.6.3.3.Red Hat Enterprise Linux Server 7;

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

3.6.3.5.CentOS-7.0;

3.6.3.6.SUSE Linux Enterprise Server 11 SP3;

3.6.3.7.SUSE Linux Enterprise Server 12;

3.6.3.8.Novell Open Enterprise Server 11 SP1;

3.6.3.9.Novell Open Enterprise Server 11 SP2;

3.6.3.10.Ubuntu Server 12.04 LTS;

3.6.3.11.Ubuntu Server 14.04 LTS;

3.6.3.12.Ubuntu Server 14.10;

3.6.3.13.Oracle Linux 6.5;

3.6.3.14.Oracle Linux 7.0;

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

3.6.3.16.openSUSE® 13.1.

3.6.4.Características:

3.6.4.1. Deve prover as seguintes proteções:

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

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

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

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

3.6.4.2.2.Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

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

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

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

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

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

3.6.4.6. Capacidade de verificar objetos usando heurística;

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

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

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

**3.7.Smartphones e tablets**

3.7.1.Compatibilidade:

3.7.1.1. Apple iOS 8.0 – 10.0;

3.7.1.2.Windows Phone 8.1 e 10;

3.7.1.3.Android OS 4.X - 7.

3.7.2.Características:

3.7.2.1.Deve prover as seguintes proteções:

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

3.7.2.1.1.1.Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

3.7.2.1.1.2.Arquivos abertos no smartphone;

3.7.2.1.1.3.Programas instalados usando a interface do smartphone

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

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

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

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

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

3.7.2.6.Capacidade de desativar por política:

3.7.2.6.1.Wi-fi;

3.7.2.6.2.Câmera;

3.7.2.6.3.Bluetooth.

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

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

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

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

3.7.2.11.Capacidade de enviar comandos remotamente de:

3.7.2.11.1.Localizar;

3.7.2.11.2.Bloquear.

3.7.2.12.Capacidade de detectar Jailbreak em dispositivos iOS;

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

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

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

3.7.2.16.Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;

3.7.2.17.Capacidade de configurar White e blacklist de aplicativos;

3.7.2.18.Capacidade de localizar o dispositivo quando necessário;

3.7.2.19.Permitir atualização das definições quando estiver em “roaming”;

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

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

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

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

3.7.2.23.1.Deletar;

3.7.2.23.2.Ignorar;

3.7.2.23.3.Quarentenar;

3.7.2.23.4.Perguntar ao usuário.

**3.8.Gerenciamento de dispositivos móveis (MDM)**

3.8.1.Compatibilidade:

3.8.1.1. Dispositivos conectados através do Microsoft Exchange ActiveSync:

3.8.1.1.1.Apple iOS;

3.8.1.1.2.Windows Phone;

3.8.1.1.3.Android.

3.8.1.2. Dispositivos com suporte ao Apple Push Notification (APNs).

3.8.1.2.1.Apple iOS 3.0 ou superior.

3.8.2.Características:

3.8.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

3.8.2.2. Capacidade de ajustar as configurações de:

3.8.2.2.1.Sincronização de e-mail;

3.8.2.2.2.Uso de aplicativos;

3.8.2.2.3.Senha do usuário;

3.8.2.2.4.Criptografia de dados;

3.8.2.2.5.Conexão de mídia removível.

3.8.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;

3.8.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS;

3.8.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

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

**3.9.Criptografia**

3.9.1.Compatibilidade:

3.9.1.1.Microsoft Windows XP Professional SP3 ou superior;

3.9.1.2. Microsoft Windows Vista Business/Enterprise/Ultimate SP2;

3.9.1.3. Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2;

3.9.1.4. Microsoft Windows 7 Professional/Enterprise/Ultimate;

3.9.1.5. Microsoft Windows 7 Professional/Enterprise/Ultimate x64;

3.9.1.6. Microsoft Windows 8 Professional/Enterprise;

3.9.1.7. Microsoft Windows 8 Professional/Enterprise x64;

3.9.1.8. Microsoft Windows 8.1 Professional / Enterprise;

3.9.1.9. Microsoft Windows 8.1 Professional / Enterprise x64;

3.9.1.10.Microsoft Windows 10 Pro x86 / x64;

3.9.1.11.Microsoft Windows 10 Enterprise x86 /x64.

3.9.2.Características:

3.9.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de

recuperação;

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

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

3.9.2.4.Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;

3.9.2.5.Permitir criar vários usuários de autenticação pré-boot;

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

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

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

3.9.2.7.2.Criptografar todos os arquivos individualmente;

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

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

3.9.2.8.Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

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

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

3.9.2.11.Verificar compatibilidade de hardware antes de aplicar a criptografia;

3.9.2.12.Possibilita estabelecer parâmetros para a senha de criptografia;

3.9.2.13.Bloqueia o reuso de senhas;

3.9.2.14.Bloqueia a senha após um número de tentativas pré-estabelecidas;

3.9.2.15.Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

3.9.2.16.Permite criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo

3.9.2.17.Permite criptografar as seguintes pastas pré-definidas: "meus documentos", "Favoritos", "Desktop", "Arquivos temporários" e "Arquivos do outlook";

3.9.2.18.Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

3.9.2.19.Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc;

3.9.2.20.Permite criar um grupo de extensões de arquivos a serem criptografados;

3.9.2.21.Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

3.9.2.22.Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

**3.10.Gerenciamento de Sistemas**

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

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

3.10.3.Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

3.10.4.Capacidade de gerenciar licenças de softwares de terceiros;

3.10.5.Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

3.10.6.Capacidade de gerenciar um inventário de hardware, com a possibilidade de

cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;

3.10.7. Possibilita fazer distribuição de software de forma manual e agendada;

3.10.8. Suporta modo de instalação silenciosa;

3.10.9. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

3.10.10. Possibilita fazer a distribuição através de agentes de atualização;

3.10.11. Utiliza tecnologia multicast para evitar tráfego na rede;

3.10.12. Possibilita criar um inventário centralizado de imagens;

3.10.13. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

3.10.14. Suporte a WakeOnLan para deploy de imagens;

3.10.15. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

3.10.16. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

3.10.17. Capacidade de gerar relatórios de vulnerabilidades e patches;

3.10.18. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

3.10.19. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

3.10.20. Permite baixar atualizações para o computador sem efetuar a instalação

3.10.21. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

3.10.22. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

3.10.23. Permite selecionar produtos a serem atualizados pela console de gerenciamento;

3.10.24.Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

**3.11.Suporte Técnico**

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

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

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

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

3.11.5.O atendimento deverá ser realizado via contato telefônico e sempre que necessário de forma on-site na sede do órgão, independentemente do tipo de incidente;

3.11.6.Suporte técnico 24x7x365, prestado unicamente à equipe de segurança da área de informática do órgão, referente a problemas de funcionamento/configuração dos produtos fornecidos;

3.11.7.Tempo de atendimento telefônico máximo de 2 (duas) horas após a abertura do chamado técnico;

3.11.8.Tempo de atendimento on-site de 6 (seis) horas após a abertura do chamado técnico;

3.11.9.Número de chamados ilimitados (remoto e on-site);

3.11.10.A contratada deverá realizar uma visita técnica on-site, 1 (uma) vez por ano, através de um técnico certificado da solução, para realizar as atualizações de versões da ferramenta e softwares como também avaliar as configurações e políticas do ambiente sempre otimizado para as boas práticas do fabricante, com carga horária de no mínimo 8 (oito) horas em horário comercial;

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

3.11.12.Severidade Nível 1 (Crítico – Onde afeta o serviço prestado da CONTRATANTE por interrupções da solução de antivírus nos sistemas operacionais, possíveis perda de

dados, alterações de configuração padrão para configuração insegura e onde não há solução alternativa disponível): 6 horas (Horário Comercial);

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

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

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

## 4. RESULTADOS ESPERADOS

- Maior capacidade e agilidade no atendimento às demandas do Tribunal de Contas;
- Proteção do parque tecnológico contra a ação das ameaças cibernéticas.

## 5. MÉTODO DE SELEÇÃO E CRITÉRIO DE AVALIAÇÃO

À luz da Lei nº 10.520/02, para efeito da concretização da formação da ARP objeto do presente Termo, será utilizado procedimento licitatório na modalidade "Pregão", na forma "eletrônica", com modo de avaliação das propostas pautado no critério do "menor preço" por item cotado.

Natal/RN, 13 de julho de 2017.

_____

Davi Ribeiro Cunha

Assessora Técnica de Informática

Matrícula 9.888-4

**PREGÃO ELETRÔNICO Nº 012/2017-TCE/RN**
**ANEXO II - MINUTA DA ATA DE REGISTRO DE PREÇO**

**ATA DE REGISTRO DE PREÇOS – ARP N° ...../2017– TCE/RN**

Aos ..... dias do mês de ..... do ano de dois mil e dezessete, o TRIBUNAL DE CONTAS DO ESTADO DO RIO GRANDE DO NORTE, com sede na Avenida Getúlio Vargas, n° 690, Bairro Petrópolis, Natal/RN, inscrito no CNPJ/MF nº 12.978.037/0001-78, neste ato representado pela Sr. Secretário Geral, Ricardo Henrique da Silva Câmara, brasileiro, casado, residente e domiciliada na Avenida Abel Cabral, 1397, Condomínio Sirius, Apartamento 1402, Torre C, Bairro Nova Parnamirim, Parnamirim – RN, CEP 59.151-250, inscrito no CPF/MF sob o nº 030.275.224-26, RG n° 1.694.214/SSP-RN, nos termos da Lei nº 8.666/93, da Lei nº 10.520/02, da Lei Complementar n° 123/2006, da Resolução nº 007/2007-TCE/RN, de 19 de julho de 2007, da Resolução nº 009/2008 – TCE, de 17 de julho de 2008, Processo nº 6933/2017, e conforme a classificação da proposta apresentada no Pregão Eletrônico nº 012/2017 – TCE/RN, homologado em __/__/2017, resolve registrar o preço oferecido pelas empresas, como segue:

| | |
|---|---|
| Empresa: | |
| CNPJ/MF n°: | Telefone: |
| Endereço: | |
| Representante Legal: | |
| RG n°: | CPF/MF n°: |

| ITEM | OBJETO | MARCA | UNIDADE | QUANTIDADE | PREÇO UNITÁRIO (R$) |
|---|---|---|---|---|---|
| | | | | | |

## 1 – DO OBJETO E DAS CONDIÇÕES

1.1 – A presente Ata tem por objeto Registro de Preços para posterior aquisição de 800 (oitocentas) licenças do software Kaspersky Endpoint Security for Business Advanced para estações de trabalho (desktops e laptops) e servidores, com criptografia de dados, segurança móvel, gerenciamento de dispositivos móveis e gerenciamento de sistemas, com atualizações para 36 meses, destinadas a atender às necessidades das Unidades Administrativas pertencentes ao TCE/RN, conforme especificações constantes no Anexo I do Edital do Pregão Eletrônico nº 012/2017 – TCE/RN (Termo de Referência) e quantidades constantes da proposta da empresa cujo preço é agora registrado.

## 2 - DA VALIDADE DOS PREÇOS

2.1 – A presente Ata de Registro de Preços terá a validade de 12 (doze) meses, contados a partir da data de sua assinatura.

2.2 – Durante o prazo de validade desta Ata de Registro de Preços, o TCE/RN não será obrigado a firmar a(s) contratação(ões) que dela poderá(ão) advir, facultando-se a realização de licitação ou de contratação direta específica para a aquisição pretendida, sendo assegurado ao beneficiário do registro preferência de fornecimento em igualdade de condições.

**3 – DO PREÇO REGISTRADO**

3.1 – O preço registrado manter-se-á fixo e irreajustável durante a validade desta Ata de Registro de Preços – ARP, ressalvadas as hipóteses previstas no art. 13 da Resolução n.º 007/2007-TCE.

**4 – DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS**

4.1 – A presente Ata de Registro de Preços poderá ser utilizada por qualquer órgão ou entidade da Administração Pública que não tenha participado do certame licitatório para sua formação, mediante autorização do Setor Gerenciador do Sistema de Registro de Preços do TCE/RN e desde que o fornecedor beneficiário da Ata, observadas as condições nela estabelecidas, opte pela aceitação do(s) fornecimento(s), independentemente dos quantitativos registrados, de modo que este(s) fornecimento(s) não prejudique(m) as obrigações anteriormente assumidas.

4.2 – O preço ofertado pela empresa signatária da presente Ata de Registro de Preços é o especificado em sua proposta de preços, anexa, de acordo com a respectiva classificação no Pregão Eletrônico nº 012/2017 – TCE/RN.

4.3 – Em cada fornecimento decorrente desta Ata, serão observadas, quanto ao preço, as cláusulas e condições constantes do Edital do Pregão Eletrônico nº 012/2017 – TCE/RN que a precedeu e a integra.

**5 - DO PRAZO E CONDIÇÕES DE ENTREGA**

5.1 – O objeto contratado com fundamento em preço registrado nesta Ata deverá ser entregue em dia com expediente no TCE/RN, de segunda à sexta-feira, das 8 às 12 horas.

5.2 – O Tribunal de Contas do Estado/RN fará as aquisições mediante emissão da Nota de Empenho específica emitida de acordo com o objeto e a quantidade determinada na respectiva solicitação.

5.3 – A Solicitação de fornecimento será enviada para a fornecedora, que deverá acusar recebimento no prazo de 01(um) dia útil.

5.4 - As quantidades e o prazo de entrega dos objetos que vierem a ser adquiridos serão definidos na respectiva Solicitação de Fornecimento, sendo o prazo máximo de entrega de 30 (trinta) consecutivos.

5.5 – Quando da entrega do objeto contratado, deverão ser observadas, obrigatoriamente, as condições previstas no Termo de Referencia que faz parte do Edital do Pregão Eletrônico nº 012/2017 – TCE/RN.

**6 - DO PAGAMENTO**

6.1 – O TCE pagará a Contratada o valor unitário constante da Proposta Comercial, multiplicado pela quantidade solicitada.

6.2 – O pagamento de cada parcela do objeto, constante da Solicitação de Fornecimento entregue e recebido em definitivo pelo TCE/RN, será efetuado por Ordem Bancária, cujo valor será creditado na Agência e Conta Corrente indicada pela Contratada, seguindo o disposto na Resolução nº 021/2016-TCE, de 6 de setembro de 2016.

**7 - DAS OBRIGAÇÕES DA CONTRATADA**

7.1. A CONTRATADA compromete-se a:

a) Fornecer o objeto desta ARP na quantidade solicitada, de acordo com as especificações técnicas constantes no Termo de Referência, pelo preço estipulado na Proposta Comercial da Adjudicatária e no prazo máximo de 30 (trinta) dias a contar do recebimento da nota de empenho;
b) Cumprir o prazo de entrega e quantidades constantes da Solicitação de Fornecimento;
c) Caso não possa cumprir os prazos estabelecidos, informar por escrito à Contratante e antes do encerramento dos prazos máximos, cabendo à Contratante definir, ou não, novo prazo.
d) Assumir a responsabilidade pelos encargos fiscais e comerciais da contratação;
e Manter, durante o período do registro de preços, em compatibilidade com as obrigações assumidas no presente instrumento, todas as condições de habilitação e qualificação exigidas na licitação, devendo comunicar ao Contratante, imediatamente, qualquer alteração que possa comprometer a manutenção da Ata de Registro de Preços referente a este certame;

**8 - DAS OBRIGAÇÕES DA CONTRATANTE**

8.1. A CONTRATANTE proporcionará à CONTRATADA todas as facilidades à boa execução do objeto desta Ata, e designará um membro da Comissão de Gerenciamento do Sistema de Registro de Preços para acompanhar o fornecimento do objeto, com a finalidade de dirimir eventuais dúvidas vinculadas ao processo;

8.2. A CONTRATANTE efetuará os pagamentos devidos nas eventuais aquisições em função da presente Ata.

**9 - DAS SANÇÕES ADMINISTRATIVAS**

9.1. Havendo atraso na entrega do objeto, sem justificativa por escrito e aceita pela CONTRATANTE, ficará sujeita à multa de 0,2% (dois décimos por cento) ao dia sobre o valor descrito na Nota de Empenho, relativo à parte entregue em atraso, a partir do dia imediato ao do vencimento do prazo até o dia da efetiva entrega do bem, observado o limite de 5% (cinco por cento).

9.2 – As multas a que se refere esta cláusula serão compensadas dos pagamentos eventualmente devidos pelo TCE/RN, ou, quando for o caso, cobradas judicialmente.

9.3 – Pela inexecução total ou parcial do contrato, o TCE/RN poderá, garantida a prévia defesa, aplicar ao contratado as seguintes sanções:

a) advertência;

b) multa, no percentual de 10% (dez por cento), calculada sobre o valor do objeto não fornecido, no caso de inexecução total ou parcial do objeto;

c) suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 2 (dois) anos;

d) declaração de inidoneidade para licitar ou contratar com a Administração Pública, facultada a defesa do interessado no prazo de 10 (dez) dias.

Parágrafo Único – A aplicação da sanção prevista na alínea "a" não prejudica a incidência cumulativa das penalidades das alíneas "b" e "c", principalmente, sem prejuízo de outras hipóteses, em caso de reincidência de atraso na entrega do objeto licitado ou caso haja cumulação de inadimplemento de eventuais cotas mensais, expressamente previstas, facultada a defesa prévia do interessado, no prazo de 05 (cinco) dias úteis.

9.4. A inexecução do contrato, de que trata o item 10.3, é configurada pelo descumprimento total ou parcial das exigências contidas no Termo de Referência.

9.5 – As sanções previstas nas alíneas "a", "c" e "d" do item 10.3 poderão ser aplicadas conjuntamente com a alínea "b", facultada a defesa prévia do interessado, no prazo de 05 (cinco) dias úteis.

9.6 – Ocorrendo a inexecução de que trata o item 10.3, reserva-se ao TCE/RN o direito de optar pela oferta que se apresentar como aquela mais vantajosa, pela ordem de classificação, comunicando-se, em seguida, o Secretário Geral, para as providências cabíveis.

9.7 – Ocorrendo a hipótese do item anterior, as adjudicatárias subseqüentes, que venham a ser convocadas, ficarão sujeitas às mesmas condições estabelecidas nesta cláusula.

9.8 – A aplicação das penalidades previstas nesta cláusula é de competência exclusiva do Secretário Geral do TCE/RN.

**10 - DAS DISPOSIÇÕES FINAIS**

10.1 – Integram esta ARP, o edital do Pregão Eletrônico nº 012/2017 – TCE/RN e seus anexos, bem como a proposta da empresa _____, vencedora do certame anteriormente referenciado.

10.2 – Os casos omissos serão resolvidos de acordo com a Resolução nº 007/2007–TCE, de 19 de julho de 2007, a Resolução nº 009/2008 – TCE, de 17 de julho de 2008, a Lei nº 10.520/02, a LC 123/2006 e, subsidiariamente, pelas normas constantes na Lei nº 8.666, de 21 de junho de 1993.

10.3 – Fica eleito o foro da Comarca de Natal/RN, capital do Estado do Rio Grande do Norte, para dirimir quaisquer dúvidas decorrentes desta Ata, com exclusão de qualquer outro, por mais privilegiado que seja.

_____
Secretário Geral

_____
Representante legal da empresa

# PREGÃO PRESENCIAL Nº 012/2017-TCE/RN
# ANEXO III - MINUTA DA ORDEM DE SERVIÇO

| *TRIBUNAL DE CONTAS DO ESTADO* | | | |
|---|---|---|---|
| ORDEM DE COMPRA | | ORDEM SERVIÇO | x |

| ORDEM N.º | DATA |
|---|---|
| | |

Processo- XXXX-XX

**PROCEDIMENTO LICITATÓRIO**

| | |
|---|---|
| INEXIGIBILIDADE..... | |
| DISPENSA..... Art. 24, inciso II, Lei nº 8.666/93..... | |
| CARTA CONVITE Nº..... | |
| TOMADA DE PREÇO Nº..... | |
| PREGÃO PRESENCIAL Nº ..... | ■ |
| CONCORRÊNCIA Nº..... | |

AUTORIZAÇÃO:

*Ricardo Henrique da Silva Câmara*
**Secretário Geral**

CONTRATANTE:
**TRIBUNAL DE CONTAS DO ESTADO DO RIO GRANDE DO NORTE**

ENDEREÇO:
AV. GETÚLIO VARGAS, 690 – PETRÓPOLIS

TELEFONE:
3642-7368

CONTRATADO:

N.º INSC. **ESTADUAL** / MUNICIPAL

ENDEREÇO:

C.N.P.J:

**SOLICITAMOS A FORNECER-NOS O MATERIAL OU PRESTAR-NOS OS SERVIÇOS ESPECIFICADOS NO VERSO**

| PRAZO DE ENTREGA: | FORMA DE PAGAMENTO: | LOCAL DE ENTREGA: |
|---|---|---|
| XX DIAS CORRIDOS A CONTAR DESTA DATA | CONTRA-EMPENHO | SEDE DO TCE / RN |

DATA:

RESPONSÁVEL: NIVALDO CORTÊS BONIFÁCIO – DIRETOR DA DAG

OBSERVAÇÕES IMPORTANTES:

1 – A presente Ordem de Compra / Serviço constitui modelo simplificado de contrato de compra e venda / prestação de serviço e foi celebrado de acordo com a parte final do artigo 62, da Lei nº 8.666, de 21 de junho de 1993.

2 – Para Qualquer esclarecimento complementar procurar o Sr. NIVALDO CORTES BONIFÁCIO, Diretor da DAG / TCE, através do telefone 3642-7370.

3 – O número desta Ordem e do Empenho devem constar, obrigatoriamente em todos os documentos do contratado.

4 – O pagamento deverá ser efetuado, através de depósito bancário em favor do CONTRATADO, na seguinte conta corrente: BANCO AG. CONTA:

5 – A despesa prevista nesta Ordem de Compra / Serviço correrá à conta de dotação orçamentária própria e específica para a sua natureza e encontra-se consignada no Orçamento Geral do Tribunal de Contas, do exercício em curso.

6 – O material adquirido ou o serviço prestado deve ser entregue acompanhado de toda a documentação fiscal necessária à liquidação da despesa.

7 – Fica acordado que ao Órgão Contratante se reserva o direito de recusar o material, obra ou serviço desta ordem, caso

não obedeça as especificações no verso, ou as constantes da respectiva licitação.

8 – Não é necessário ao fornecedor requerer o pagamento desta contratação.

| ITEM | E S P E C I F I C A Ç Õ E S | UNIDADE | QUANTIDADE | P R E Ç O S | |
|---|---|---|---|---|---|
| | | | | UNITÁRIO | TOTAL |
| | | | | | |
| **Importa a presente Ordem de Serviço o valor de R$ XX (XXXXXX).** | | | | **TOTAL** | **R$ XXXXXX** |

**PREGÃO ELETRÔNICO Nº 012/2017-TCE/RN**
**ANEXO IV - MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE TRABALHADOR DE MENOR**

(nome da empresa)_____, inscrito(a) no CNPJ n°_____, por intermédio de seu representante legal o(a) Sr(a)_____, portador(a) da Carteira de Identidade nº..... e do CPF nº ....., DECLARA, para fins do disposto no item inciso V do art. 27 da Lei no 8.666, de 21 de junho de 1993, acrescido pela Lei nº 9.854, de 27 de outubro de 1999, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz (  ).
*(Local e data)*

_____
(representante legal)

**PREGÃO ELETRÔNICO Nº 012/2017-TCE/RN**
**ANEXO V – MODELO DE PROPOSTA DE PREÇO**

(Papel timbrado da Licitante)
Proposta que faz a empresa _____, inscrita no CNPJ/MF sob o nº _____e inscrição estadual nº _____, estabelecida no (a)_____(endereço completo), para aquisição de licenças do software Kaspersky Endpoint Security for Business Advanced, conforme estabelecido no Pregão Eletrônico nº 012/2017-TCE/RN.

Os nossos preços ofertados na presente licitação são os constante do quadro a seguir:

| ITEM | DISCRIMINAÇÃO DO PRODUTO | QUANT | PREÇO UNITÁRIO | PREÇO TOTAL |
|---|---|---|---|---|
| 01 | Aquisição de licenças do software Kaspersky Endpoint Security for Business Advanced, conforme o edital do Pregão Eletrônico nº 012/2017 e seus anexos. | 800 | | |

Declaramos, expressamente, que concordamos, integralmente e sem qualquer restrição, com as condições da contratação.

VALIDADE DA PROPOSTA
(60) Sessenta dias, no mínimo.

BANCO: ..... – AGÊNCIA: ..... – CONTA: .....;
Representante Legal:
RG n°:
CPF/MF n°:

Atenciosamente,

Local e data:

_____
(Nome e assinatura do representante legal)