PREGÃO ELETRÔNICO Nº 10/2023

Torna-se público que **TRIBUNAL DE CONTAS DO ESTADO DO RIO GRANDE DO NORTE – TCE/RN**, sediado na Av. Getúlio Vargas, 690, Petrópolis, Natal/RN, por meio da sua Pregoeira, designada pela Portaria nº 022/2023-GP/TCE, de 16 de janeiro de 2023, publicada no Diário Eletrônico do TCE/RN, edição de 16 de janeiro de 2023, realizará licitação na modalidade **PREGÃO**, na forma **ELETRÔNICA,** do tipo **MENOR PREÇO,** nos termos da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 10.024, de 20 de setembro de 2019, da Resolução 009/2008-TCE, de 17 de julho de 2008, da Resolução 007/2007-TCE, de 19 de julho de 2007, da Lei Complementar n° 123, de 14 de dezembro de 2006, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993 e as exigências estabelecidas neste Edital.

DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO
Data da sessão: 15 de agosto de 2023
Horário: 09 hr (horário de Brasília)
Local: Portal de Compras do Governo Federal – www.comprasgovernamentais.gov.br
Processo Administrativo: 1600/2023
UASG: 925468

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. O objeto da presente licitação é a **formação de Ata de Registro de Preços para posterior aquisição de 700 (setecentas) licenças do software Kaspersky Endpoint Security for Business Advanced (PLUS) e aquisição de 10 (dez) licenças Kaspersky Hybrid Cloud Security CPU (PLUS), com direito a atualizações pelo período de 36 (trinta e seis) meses destinadas a atender às necessidades das Unidades Administrativas pertencentes ao TCE/RN,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em **grupo único, formados por 2 itens**, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

1.3. O critério de julgamento adotado será o **menor preço GLOBAL do grupo**, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

2. 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.compras.gov.br.

2.3. 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. DOS RECURSOS ORÇAMENTÁRIOS

3.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento desta Corte para o exercício de 2021, na classificação:

3.1.1 Unidade Orçamentária: 02101 - Tribunal de Contas do Estado - TCE
3.1.2. Sub-Função: 202101 – MANUTENÇÃO E FUNCIONAMENTO
3.1.3. Natureza da Despesa: 33 – Despesas Correntes.
3.1.4. Elemento: 33.90.40 – Serviços de Tec. Da Informação e comunicação – Pessoa Jurídica
3.1.5. Fonte de Recursos: 0.500 - Recursos Ordinários.

4. DO CREDENCIAMENTO

4.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

4.1.1. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.compras.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

4.2. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

4.3. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

4.4. É de responsabilidade exclusiva do licitante o uso adequado do sistema, cabendo-lhe zelar por todas as transações efetuadas diretamente ou por seu representante.

4.5. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

4.5.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação

5. DA PARTICIPAÇÃO NO PREGÃO.

5.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

5.2. Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.

5.3. Será concedido tratamento favorecido para as MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE, para as sociedades cooperativas mencionadas no artigo 34 da Lei nº 11.488, de 2007 e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

5.4. Não poderão participar desta licitação os interessados:

a. proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

b. que não atendam às condições deste Edital e seu(s) anexo(s);

c. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

d. que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

e. que estejam sob falência, concurso de credores, concordata ou em processo de dissolução ou liquidação;

f. entidades empresariais que estejam reunidas em consórcio;

5.5. 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.

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

6. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

6.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

6.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

6.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

6.4. No caso de haver divergência entre a descrição do código dos produtos no COMPRASNET e o disposto no Anexo I – Termo de Referência, o licitante deverá obedecer a este último.

6.5. As MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

6.5. Incumbirá ao 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 quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

6.6. Até a abertura da sessão, os licitantes poderão retirar ou substituir as propostas e os documentos de habilitação anteriormente inseridos no sistema;

6.7. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

6.8. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação da Pregoeira e para acesso público após o encerramento do envio de lances.

6.8.1 Somente serão aceitos documentos legíveis.

6.9. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.9.1. Valor unitário e total;

6.9.2. Marca;

6.9.3. Fabricante;

6.9.4. Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência.

6.9.4.1. Caso a proposta seja omissa, considerar-se-á que as suas especificações serão as que constam do **Anexo I – Termo de Referência** deste Edital

6.10. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.

6.11. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

6.12. Qualquer elemento que possa identificar à licitante no preenchimento do campo Proposta do sistema importa a desclassificação da proposta.

6.13. O prazo de validade da proposta não será inferior a **60 (sessenta) dias,** a contar da data de sua apresentação.

6.13.1. Decorrido o prazo de validade das propostas, sem convocação para contratação, ficam as licitantes liberadas dos compromissos assumidos.

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

a. 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 – Termo de Referência** deste Edital;

b. prazo para entrega de no máximo 30 (trinta) dias corridos, contados a partir da data de recebimento da Ordem de Compra por parte do licitante vencedor;

7. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

7.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

7.2. A Pregoeira verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

7.2.1. Também será desclassificada a proposta que identifique o licitante.

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

7.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

7.4. O sistema disponibilizará campo próprio para troca de mensagens entre a Pregoeira e os licitantes.

7.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.5.1. O lance deverá ser ofertado pelo valor total do lote.

7.5.2. Não poderá haver desistência dos lances ofertados, sujeitando-se a proponente desistente às penalidades previstas no artigo 49 do Decreto nº 10.024/19.

7.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.7. O licitante somente poderá oferecer lance inferior ao último por ele ofertado e registrado pelo sistema.

7.8. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 0,1 (um centavo).

7.9. O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20) segundos e o intervalo entre lances não poderá ser inferior a três (3) segundos, sob pena de serem automaticamente descartados pelo sistema os respectivos lances.

7.10. Será adotado para o envio de lances no pregão eletrônico o **modo de disputa "aberto e fechado"**, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

7.11. A etapa de lances da sessão pública terá duração inicial de quinze (15) minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até dez (10) minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

7.12. Encerrado o prazo previsto no item anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até dez por cento (10%) superiores àquela possam ofertar um lance final e fechado em até cinco (5) minutos, o qual será sigiloso até o encerramento deste prazo.

7.13. Não havendo pelo menos três (3) ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três (3), oferecer um lance final e fechado em até cinco (5) minutos, o qual será sigiloso até o encerramento deste prazo.

7.14. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará os lances segundo a ordem crescente de valores.

7.15. Não havendo lance final e fechado classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada, para que os demais licitantes, até o máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

7.16. Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atender às exigências de habilitação.

7.17. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

7.18. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

7.19. Quando a desconexão do sistema eletrônico para a Pregoeira persistir por tempo superior a dez (10) minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro (24) horas da comunicação do fato pela Pregoeira aos participantes, no sítio eletrônico utilizado para divulgação.

7.20. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

7.21. Só se considera empate entre propostas iguais, não seguidas de lances. Lances equivalentes não serão considerados iguais, uma vez que a ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação.

7.22. Havendo eventual empate entre propostas, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando a preferência.

7.23. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

7.24. Encerrada a etapa de envio de lances da sessão pública, a Pregoeira deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

7.25. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.26. Após a negociação do preço, a Pregoeira iniciará a fase de aceitação e julgamento da proposta.

8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

8.1. Encerrada a etapa de negociação, a Pregoeira examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

8.2. Não serão aceitas propostas com valor unitário superior ao estimado ou com preços manifestamente inexequíveis.

8.2.1. Os critérios de aceitabilidade são cumulativos, verificando-se tanto o valor global quanto os valores unitários estimativos da contratação.

8.2.2. Considerar-se-á inexequível a proposta que não venha a ser demonstrada sua viabilidade por meio de documentação que comprove que os custos envolvidos na contratação são coerentes com os de mercado do objeto deste Pregão. O ônus da prova da exeqüibilidade dos preços cotados incumbe ao autor da proposta, no prazo estipulado pela Pregoeira, contados da intimação.

8.2.3. As propostas com valor unitário superior ao estimado poderão ser aceitas, caso houver justificativa expressa do Setor Demandante e/ou da Pregoeira.

8.3. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro (24) horas de antecedência.

8.4. Se a proposta ou lance vencedor for desclassificado, a Pregoeira examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação e poderá negociar com o licitante para que seja obtido preço melhor.

8.5. Encerrada a análise quanto à aceitação da proposta, a Pregoeira verificará a habilitação do licitante, observado o disposto neste Edital.

9. AMOSTRA

9.1. A Pregoeira poderá convocar o licitante para enviar documento digital, por meio de funcionalidade disponível no sistema, estabelecendo no "chat" prazo razoável para tanto, sob pena de não aceitação da proposta.

9.1.1. Dentre os documentos passíveis de solicitação pela Pregoeira, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos ou folhetos, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pela Pregoeira, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

9.1.1.1. O prazo estabelecido pela Pregoeira poderá ser prorrogado por solicitação escrita e justificada do licitante, pelo e-mail **pregaotce@gmail.com**, formulada antes de findo o prazo estabelecido, e formalmente aceita pela Pregoeira.

9.2. Caso a compatibilidade com as especificações demandadas, sobretudo quanto a padrões de qualidade e desempenho, não possa ser aferida pelos meios previstos nos subitens acima, ou a critério do Setor Demandante, a Pregoeira exigirá que o licitante classificado em primeiro lugar apresente amostra, sob pena de não aceitação da proposta, no local a ser indicado e dentro de **5 (cinco) dias úteis** contados da solicitação. A Pregoeira suspenderá a sessão, informando no "*chat*" a nova data e horário para a sua continuidade.

9.2.1. 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 pelo e-mail pregaotce@gmail.com** dentro do prazo estabelecido.

9.2.1.1. A Pregoeira poderá solicitar via "chat" o comprovante do envio do produto por empresa transportadora ou Correio na reabertura da sessão, dando um prazo de 15 minutos para o envio através do email pregaotce@gmail.com.

9.3. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

9.3.1. A apresentação de amostra falsificada ou deteriorada, como original ou perfeita, configura comportamento inidôneo, punível nos termos deste Edital.

9.4. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pela Pregoeira, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

9.5. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), a Pregoeira analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

9.6. Os exemplares colocados à disposição da Administração serão tratados como protótipos, podendo ser manuseados e desmontados pela equipe técnica responsável pela análise, não gerando direito a ressarcimento.

9.7. Após a divulgação do resultado final da licitação, as amostras entregues deverão ser recolhidas pelos licitantes no **prazo de 5 (cinco) dias utéis**, após o qual poderão ser descartadas pela Administração, sem direito a ressarcimento.

9.8. Os licitantes deverão colocar à disposição da Administração todas as condições indispensáveis à realização de testes e fornecer, sem ônus, os manuais impressos em língua portuguesa, necessários ao seu perfeito manuseio, quando for o caso.

10. HABILITAÇÃO

10.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, a Pregoeira verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

10.1.1. SICAF;
10.1.2. Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (https://certidoes-apf.apps.tcu.gov.br/)

10.1.3. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

10.1.3.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

10.1.3.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

10.1.3.3. O licitante será convocado para manifestação previamente à sua desclassificação.

10.1.4. Constatada a existência de sanção, a Pregoeira reputará o licitante inabilitado, por falta de condição de participação.

10.2. Caso atendidas as condições de participação, a habilitação do licitantes será verificada por meio do SICAF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e habilitação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

10.2.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas;

10.2.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

10.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, **salvo se houver, por parte da Pregoeira, consulta aos sítios eletrônicos oficiais emissores de certidões com a obtenção(ões) da(s) certidão(ões) válida(s)**, conforme art. 43, §3º, do Decreto 10.024, de 2019.

10.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no **prazo de 2 (duas) horas**, sob pena de inabilitação.

10.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

10.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.6.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

10.7. Ressalvado o disposto no item 6.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação:

10.8. Habilitação Jurídica

10.8.1. registro comercial, no caso de empresa individual (Requerimento de Empresário);

10.8.2. Em se tratando de MICROEMPREENDEDOR INDIVIDUAL – MEI: Certificado da Condição de MICROEMPREENDEDOR INDIVIDUAL - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

10.8.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

10.8.4. inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

10.8.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

10.8.6. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

10.9. Qualificação Técnica

10.9.1. Atestado de capacidade técnica – no mínimo 01 (um) – exclusivamente em nome da licitante, expedidos por pessoa jurídica de direito público ou privado,

comprovando já ter executado ou estar prestando a contento, serviços compatíveis com o objeto da licitação.

10.10. Qualificação Econômica-Financeira

10.10.1. Certidão Negativa de Falência ou Recuperação Judicial expedida pelo Distribuidor da sede da Licitante.

10.10.2. 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;

10.10.2.2 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;

10.10.2.3 É admissível o balanço intermediário, se decorrer de lei ou contrato social/estatuto social.

10.10.3. 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:

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

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

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

10.10.4. 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.

10.11. Regularidade Fiscal e Trabalhista

10.11.1 Comprovante de Inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ, expedido pela Receita Federal;

10.11.2. Certidão de Regularidade do FGTS - CRF, emitido pela Caixa Econômica Federal;

10.11.3. 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 com a Receita Federal do Brasil;

10.11.4. Certidão Negativa (ou positiva com efeito de negativa) de Débito do Estado do domicílio ou sede do licitante;

10.11.5. Certidão Negativa (ou positiva com efeito de negativa) de Débito do Município do domicílio ou sede do licitante;

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

10.12. O licitante enquadrado como MICROEMPREENDEDOR INDIVIDUAL que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

10.13. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como MICROEMPRESA OU EMPRESA DE PEQUENO PORTE seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

10.13.1. Uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista da MICROEMPRESA OU EMPRESA DE PEQUENO PORTE, a mesma será convocada para, no **prazo de 5 (cinco) dias úteis**, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

10.14. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se seguir-se outra MICROEMPRESA OU EMPRESA DE PEQUENO PORTE com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

10.15. Havendo necessidade de analisar minuciosamente os documentos exigidos, a Pregoeira suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

10.16. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ilegíveis ou apresentá-los em desacordo com o estabelecido neste Edital.

10.17. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

11. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

11.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de **24 (vinte e quatro) horas**, a contar da solicitação da Pregoeira no sistema para o **e-mail pregaotce@gmail.com** e deverá:

11.1.1. Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, com as informações estabelecidas no item 6.9 e devendo a última folha ser assinada e as demais rubricadas pelo seu representante legal.

11.1.2. Conter a indicação do banco, da agência e da conta corrente da empresa licitante e a indicação da pessoa legalmente responsável pela empresa, assim como o telefone e e-mail para contato.

11.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

11.2.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

11.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

11.3.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

11.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

11.5. Não caberá desistência da proposta, salvo por motivo justo, decorrente de fator superveniente e aceito pela Pregoeira.

12. DOS RECURSOS

12.1. Declarado o vencedor será concedido o **prazo de 30 (trinta) minutos**, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

12.2. Havendo quem se manifeste, caberá à Pregoeira verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

12.2.1. Nesse momento a Pregoeira não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

12.2.2. Uma vez admitido o recurso, o recorrente terá, a partir de então, o **prazo de 3 (três) dias** para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros **3 (três) dias**, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

12.2.3. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

12.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. A sessão pública poderá ser reaberta:

13.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

13.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

13.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

13.2.1. A convocação se dará por meio do sistema eletrônico ("chat" ou "Aviso") ou e-mail, de acordo com a fase do procedimento licitatório.

13.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

14. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

14.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato da Pregoeira, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

14.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

15. DA GARANTIA DE EXECUÇÃO

15.1. Não haverá exigência de garantia de execução para a presente contratação.

16. DA ATA DE REGISTRO DE PREÇOS

16.1. Homologado o resultado da licitação, terá o adjudicatário o **prazo de 5 (cinco) dias**, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

16.2. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura da Ata de Registro de Preços, a Administração poderá encaminhá-la para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinada e devolvida no **prazo de 7 (sete) dias**, a contar da data de seu recebimento.

16.3. O prazo estabelecido no subitem anterior para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo(s) licitante(s) vencedor(s), durante o seu transcurso, e desde que devidamente aceito pela autoridade competente.

16.3.1. Serão formalizadas tantas Atas de Registro de Preços quanto necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do

licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

17. DO CONTRATO

17.1. Conforme preceitua o art. 62, parágrafo 4º da Lei Federal nº 8.666/93, o termo de contrato será substituído pela a Ordem de Compra.

18. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

18.1. Os critérios de aceitação do objeto e de fiscalização estão previstos no **Anexo I – Termo de Referência** e **Anexo IV - Ordem de Compra** deste Edital.

19. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

19.1. As obrigações da Contratante e da Contratada são as estabelecidas no **Anexo I – Termo de Referência** e **Anexo IV - Ordem de Compra** deste Edital.

20. DO PAGAMENTO

20.1. As regras acerca do reajuste do valor contratual são as estabelecidas no **Anexo IV - Ordem de Compra** deste Edital.

21. DAS SANÇÕES ADMINISTRATIVAS

21.1. As sanções administrativas estão elencadas no **Anexo IV - Ordem de Compra** deste Edital.

22. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

22.1. Até 3 (três) dias úteis antes da data designada para abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

22.2. A impugnação poderá ser realizada por forma eletrônica pelo e-mail **pregaotce@gmail.com**

22.3. Caberá a Pregoeira, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação **no prazo de até 02 (dois) dias úteis** contados da data de recebimento da impugnação.

22.4. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

22.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados a Pregoeira, **até 03 (três) dias úteis anteriores** à data designada para abertura

da sessão pública, exclusivamente por meio eletrônico, pelo e-mail **pregaotce@gmail.com**

22.6. A Pregoeira responderá aos pedidos de esclarecimentos no **prazo de 02 (dois) dias úteis**, contado da data de recebimento do pedido, e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos.

22.7. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

22.7.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pela Pregoeira, nos autos do processo de licitação.

22.8. As respostas às impugnações e os esclarecimentos prestados pela Pregoeira serão disponibilizadas no sistema eletrônico para os interessados, bem como vincularão os participantes e a administração.

23. DAS DISPOSIÇÕES GERAIS

23.1. À autoridade competente, na defesa do interesse do serviço público e de acordo com a legislação vigente, reserva-se o direito de anular ou revogar, no todo ou em parte, a presente licitação.

23.1.1. A anulação do Pregão induz à Ordem de Compra.

23.2. A homologação do resultado desta licitação não implicará direito à contratação.

23.3. 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 8h às 18h, de segunda a quinta-feira, e das 7h às 13h, na sexta-feira (horário local).

23.4. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

23.5. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

23.6. É facultado à Pregoeira ou à autoridade superior, em qualquer fase deste Pregão, promover diligência destinada a esclarecer ou completar a instrução do processo, vedada a inclusão posterior de informação ou de documentos que deveriam ter sido apresentados para fins de classificação e habilitação.

23.7. No julgamento das propostas e da habilitação, a Pregoeira poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade

jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

23.8. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

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

23.10. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

23.11. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

23.12. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

23.13. 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, do Decreto nº 10.024, de 20 de setembro de 2019, a LC 123/2006, da Resolução nº 009/2008-TCE/RN, de 17 de julho de 2008, e, subsidiariamente, das normas constantes da Lei nº 8.666, de 21 de junho de 1993, com as devidas alterações.

23.14. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

22.14.1. ANEXO I - Termo de Referência;

22.14.2. ANEXO II – Modelo de Proposta de Preço;

22.14.3. ANEXO III – Ata de Registro de Preço;

22.14.4. ANEXO IV - Ordem de Compra.

Natal (RN), 02 de agosto de 2023.

assinado eletronicamente
Vanessa de Sousa Menezes Ubarana
Pregoeira

ANEXO I – TERMO DE REFERÊNCIA

TERMO DE REFERÊNCIA

1. OBJETIVO

1.1. A formação de Ata de Registro de Preços (ARP) para posterior aquisição de 700 (setecentas) licenças do software Kaspersky Endpoint Security for Business Advanced (PLUS) e aquisição de 10 (dez) licenças Kaspersky Hybrid Cloud Security CPU (PLUS), com direito a atualizações pelo período de 36 (trinta e seis) meses destinadas a atender às necessidades das Unidades Administrativas pertencentes ao TCE/RN.

2. JUSTIFICATIVA DA AQUISIÇÃO

2.1. 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.

2.2. A escolha da solução Kaspersky Endpoint Security for Business Advanced se deu por já ser a solução utilizada pelo TCE/RN, razão pela qual só estamos buscando as licenças, que estão prestes a vencer (23 de setembro de 2023), com intuito de baratear a aquisição, conforme o princípio da economicidade.

2.3. De acordo ainda com o princípio da economicidade, esclarecemos que não estamos solicitando serviços extras, nem solicitando qualquer tipo de treinamento que seria necessário caso fosse licitado para outras soluções disponíveis no mercado. Além disso, a equipe atual de infraestrutura de TI do TCE/RN já possui conhecimento técnico para operacionalizar a versão Kaspersky Endpoint Security for Business Advanced.

3. PRODUTO

3.1. Os produtos, objeto da composição do registro de preços em referência, corresponde ao item discriminado e devidamente especificado, conforme se segue:

LOTE	ITEM	QTD	DESCRIÇÃO
1	1	700	Kaspersky endpoint security for business advanced (PLUS), pelo período de 36 meses.
1	2	10	Kaspersky Hybrid Cloud Security CPU Standard (PLUS), pelo período de 36 meses.

ITEM 1 - KASPERSKY ENDPOINT SECURITY FOR BUSINESS ADVANCED (PLUS):

4. ESPECIFICAÇÃO TÉCNICA

4.1. Características Gerais

4.1.1. Todas as licenças fornecidas terão validade de 36 (trinta e seis) meses para atualizações inerentes ao produto;

4.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus, quanto do software;

4.1.3. As atualizações deverão ser disponibilizadas através de site na Internet, ou através do próprio software;

4.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para a CONTRATADA além daquele já cotado na proposta;

4.2. SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA

4.2.1. Compatibilidade:

4.2.1.1. Microsoft Windows Server 2008 (Todas edições);

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

4.2.1.3. Microsoft Windows Server 2012 (Todas edições x64);

4.2.1.4. Microsoft Windows Server 2012 R2 (Todas edições x64);

4.2.1.5. Microsoft Windows Server 2016 x64;

4.2.1.6. Windows Server 2019 x64;

4.2.1.7. Windows Server 2022 x64;

4.2.1.8. Microsoft Windows 8 Professional / Enterprise x64;

4.2.1.9. Microsoft Windows 8.1 Professional / Enterprise x86;

4.2.1.10. Microsoft Windows 8.1 Professional / Enterprise x64;

4.2.1.11. Microsoft Windows 10 (Todas edições x86);

4.2.1.12. Microsoft Windows 10 (Todas edições x64);

4.2.1.13. Microsoft Windows 11 (Todas edições x86);

4.2.1.14. Microsoft Windows 11 (Todas edições x64).

4.2.2. Características:

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

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

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

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

4.2.2.5. Deve permitir incluir usuários do AD para logarem na console de administração;

4.2.2.6. Possuir recurso de controle de acesso baseado em funções (RBAC);

4.2.2.7. 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;

4.2.2.8. 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;

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

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

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

4.2.2.12. Possuir integração com ferramentas de SIEM (Security Information and Event Management) utilizando protocolo syslog;

4.2.2.13. Deve armazenar histórico das alterações feitas em políticas;

4.2.2.14. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

4.2.2.15. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

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

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

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

4.2.2.19. Capacidade de instalar remotamente qualquer "app" em smartphones e tablets de sistema iOS;

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

4.2.2.21. 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;

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

4.2.2.23. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

4.2.2.24. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

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

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

4.2.2.27. 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;

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

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

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

4.2.2.31. Nome do computador;

4.2.2.32. Nome do domínio;

4.2.2.33. Range de IP;

4.2.2.34. Sistema Operacional;

4.2.2.35. Máquina virtual.

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

4.2.2.37. 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;

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

4.2.2.39. 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;

4.2.2.40. 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;

4.2.2.41. 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;

4.2.2.42. 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;

4.2.2.43. Deve fornecer as seguintes informações dos computadores:

4.2.2.44. Se o antivírus está instalado;

4.2.2.45. Se o antivírus está iniciado;

4.2.2.46. Se o antivírus está atualizado;

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

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

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

4.2.2.50. Versão do antivírus instalado na máquina;

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

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

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

4.2.2.54. Nome do computador;

4.2.2.55. Domínio ou grupo de trabalho do computador;

4.2.2.56. Data e horário da última atualização de vacinas;

4.2.2.57. Sistema operacional com Service Pack;

4.2.2.58. Quantidade de processadores;

4.2.2.59. Quantidade de memória RAM;

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

4.2.2.61. Endereço IP;

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

4.2.2.63. Atualizações do Windows Updates instaladas;

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

4.2.2.65. Vulnerabilidades de aplicativos instalados na máquina;

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

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

4.2.2.68. Alteração de Gateway Padrão;

4.2.2.69. Alteração de subrede;

4.2.2.70. Alteração de domínio;

4.2.2.71. Alteração de servidor DHCP;

4.2.2.72. Alteração de servidor DNS;

4.2.2.73. Alteração de servidor WINS;

4.2.2.74. Alteração de subrede;

4.2.2.75. Resolução de Nome;

4.2.2.76. Disponibilidade de endereço de conexão SSL;

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

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

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

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

4.2.2.81. 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;

4.2.2.82. 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;

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

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

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

4.2.2.86. Listar em um único local, todos os computadores não gerenciados na rede;

4.2.2.87. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

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

4.2.2.89. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;

4.2.2.90. 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;

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

4.2.2.92. Deve através de opções de otimização fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;

4.2.2.93. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

4.2.2.94. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;

4.2.2.95. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados

na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

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

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

4.2.2.97.1. Nome do vírus;

4.2.2.97.2. Nome do arquivo infectado;

4.2.2.97.3. Data e hora da detecção;

4.2.2.97.4. Nome da máquina ou endereço IP;

4.2.2.97.5. Ação realizada.

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

4.2.2.99. Capacidade de listar updates nas máquinas com o respectivo link para download;

4.2.2.100. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;

4.2.2.101. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

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

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

4.2.2.104. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

4.3. ESTAÇÕES WINDOWS

4.3.1. Compatibilidade:

4.3.1.1. Microsoft Windows 7 Professional/Enterprise/Ultimate;

4.3.1.2. Microsoft Windows 8 Professional/Enterprise;

4.3.1.3. Microsoft Windows 8.1 Professional/Enterprise;

4.3.1.4. Microsoft Windows 10 Professional/Enterprise.

4.3.1.5. Microsoft Windows 11 Professional/Enterprise.

4.3.2. Características:

4.3.2.1. Deve prover as seguintes proteções:

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

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

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

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

4.3.2.6. Firewall com IDS;

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

4.3.2.8. Controle de dispositivos externos;

4.3.2.9. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

4.3.2.10. Controle de acesso a sites por horário;

4.3.2.11. Controle de acesso a sites por usuários;

4.3.2.12. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;

4.3.2.13. Controle de execução de aplicativos;

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

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

4.3.2.16. 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);

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

4.3.2.18. 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;

4.3.2.19. 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;

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

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

4.3.2.22. 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;

4.3.2.23. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

4.3.2.24. Capacidade de verificar somente arquivos novos e alterados;

4.3.2.25. Capacidade de verificar objetos usando heurística;

4.3.2.26. Capacidade de agendar uma pausa na verificação;

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

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

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

4.3.2.30. Perguntar o que fazer, ou;

4.3.2.31. Bloquear acesso ao objeto;

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

4.3.2.33. Caso positivo de desinfecção:

4.3.2.34. Restaurar o objeto para uso;

4.3.2.35. Caso negativo de desinfecção:

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

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

4.3.2.38. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

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

4.3.2.40. Capacidade de verificar tráfego nos browsers: Microsoft Edge, Firefox, Google Chrome e Opera;

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

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

4.3.2.42.1. Perguntar o que fazer, ou;

4.3.2.42.2. Bloquear o e-mail;

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

4.3.2.42.4. Caso positivo de desinfecção:

4.3.2.42.5. Restaurar o e-mail para o usuário;

4.3.2.42.6. Caso negativo de desinfecção:

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

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

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

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

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

4.3.2.46. Deve ter suporte total ao protocolo Ipv6;

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

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

4.3.2.49. Perguntar o que fazer, ou;

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

4.3.2.51. Permitir acesso ao objeto;

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

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

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

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

4.3.2.56. 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;

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

4.3.2.58. 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;

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

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

4.3.2.61. 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;

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

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

4.3.2.64. 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.

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

4.3.2.65.1. Discos de armazenamento locais;

4.3.2.65.2. Armazenamento removível;

4.3.2.65.3. Impressoras;

4.3.2.65.4. CD/DVD;

4.3.2.65.5. Drives de disquete;

4.3.2.65.6. Modems;

4.3.2.65.7. Dispositivos de fita;

4.3.2.65.8. Dispositivos multifuncionais;

4.3.2.65.9. Leitores de smart card;

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

4.3.2.65.11. Wi-Fi;

4.3.2.65.12. Adaptadores de rede externos;

4.3.2.65.13. Dispositivos MP3 ou smartphones;

4.3.2.65.14. Dispositivos Bluetooth;

4.3.2.65.15. Câmeras e Scanners.

4.3.2.66. 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;

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

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

4.3.2.69. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.

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

4.3.2.71. 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);

4.3.2.72. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

4.3.2.73. Blacklist: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

4.3.2.74. Whitelist: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

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

4.3.2.76. 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;

4.3.2.77. 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;

4.3.2.78. 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.

4.3.2.79. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

4.3.2.80. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

4.3.2.81. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

4.3.2.82. Capacidade de integração com o Windows Defender Security Center.

4.3.2.83. Capacidade de integração com a Antimalware Scan Interface (AMSI).

4.3.2.84. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

4.3.2.85. Deve possuir módulo que monitora e bloqueia atividades potencialmente maliciosas, baseado no comportamento do usuário e Machine Learning.

4.3.2.86. O módulo deve ser capaz de agir nos seguintes estados:

4.3.2.86.1. Aprendizado: coleta informações sobre as atividades executadas pelo usuário.

4.3.2.86.2. Bloqueio: bloqueia as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.

4.3.2.86.3. Notificação: notifica sobre as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.

4.4. ESTAÇÕES MAC OS X

4.4.1. Compatibilidade:

4.4.1.1. Apple macOS;

4.4.1.2. Apple Mac OS X.

4.4.2. Características:

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

4.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https;

4.4.2.3. Possuir módulo de bloqueio a ataques na rede;

4.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

4.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;

4.4.2.6. Possibilidade de importar uma chave no pacote de instalação;

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

4.4.2.8. Deve possuir suportes a notificações utilizando o Growl;

4.4.2.9. 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);

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

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

4.4.2.12. 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;

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

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

4.4.2.15. Capacidade de verificar somente arquivos novos e alterados;

4.4.2.16. Capacidade de verificar objetos usando heurística;

4.4.2.17. Capacidade de agendar uma pausa na verificação;

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

4.4.2.19. Perguntar o que fazer, ou;

4.4.2.20. Bloquear acesso ao objeto;

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

4.4.2.20.2. Caso positivo de desinfecção:

4.4.2.20.3. Restaurar o objeto para uso;

4.4.2.20.4. Caso negativo de desinfecção:

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

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

4.4.2.22. Capacidade de verificar arquivos de formato de email;

4.4.2.23. 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;

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

5. ESTAÇÕES DE TRABALHO LINUX

5.1. Compatibilidade:

5.1.1. Plataforma 32-bits:

5.1.1.1. Ubuntu;

5.1.1.2. Red Hat® Enterprise Linux®;

5.1.1.3. CentOS;

5.1.1.4. Fedora;

5.1.1.5. Debian GNU / Linux.

5.1.2. Plataforma 64-bits:

5.1.2.1. Ubuntu;

5.1.2.2. Red Hat Enterprise Linux;

5.1.2.3. CentOS;

5.1.2.4. Fedora;

5.1.2.5. Debian GNU / Linux;

5.1.2.6. OracleLinux;

5.1.2.7. SUSE® Linux Enterprise Server;

5.1.2.8. openSUSE®.

5.2. Características:

5.2.1. Deve prover as seguintes proteções:

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

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

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

5.2.5. Capacidade de criar exclusões por local, máscara e nome da ameaça;

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

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

5.2.8. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

5.2.9. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

5.2.9.1. Alta;

5.2.9.2. Média;

5.2.9.3. Baixa;

5.2.9.4. Recomendado;

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

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

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

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

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

5.2.15. Capacidade de verificar objetos usando heurística;

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

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

5.2.18. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados; de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

6. SERVIDORES WINDOWS

6.1. Compatibilidade:

6.1.1. Microsoft Windows Server 2003 Standard / Enterprise / Datacenter SP2 (x32 / x64);

6.1.2. Microsoft Windows Server 2003 R2 Standard/ Enterprise / Datacenter SP2 (x32/ x64);

6.1.3. Microsoft Windows Server 2008 R2 Standard / Enterprise x64 SP1;

6.1.4. Microsoft Windows Server 2008 Standard / Enterprise SP2;

6.1.5. Microsoft Windows Server 2008 Standard / Enterprise x64 SP2;

6.1.6. Microsoft Windows Server 2012 Standard / Foundation / Essentials x64;

6.1.7. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64;

6.1.8. Microsoft Windows Server 2016;

6.1.9. Microsoft Windows Server 2019;

6.1.10. Microsoft Windows Server 2022.

6.2. Características:

6.2.1. Deve prover as seguintes proteções:

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

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

6.2.4. Firewall com IDS;

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

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

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

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

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

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

6.2.11. Leitura de configurações;

6.2.12. Modificação de configurações;

6.2.13. Gerenciamento de Backup e Quarentena;

6.2.14. Visualização de relatórios;

6.2.15. Gerenciamento de relatórios;

6.2.16. Gerenciamento de chaves de licença;

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

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

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

6.2.20. 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.

6.2.21. 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;

6.2.22. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;

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

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

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

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

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

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

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

6.2.30. 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;

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

6.2.32. 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;

6.2.33. Capacidade de verificar somente arquivos novos e alterados;

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

6.2.35. Capacidade de verificar objetos usando heurística;

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

6.2.37. Capacidade de agendar uma pausa na verificação;

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

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

6.2.40. Perguntar o que fazer, ou;

6.2.41. Bloquear acesso ao objeto;

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

6.2.41.2. Caso positivo de desinfecção:

6.2.41.3. Restaurar o objeto para uso;

6.2.41.4. Caso negativo de desinfecção:

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

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

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

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

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

6.2.46. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

6.2.47. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning);

6.2.48. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

7. SERVIDORES LINUX

7.1. Compatibilidade:

7.1.1. Plataforma 32-bits:

7.1.1.1. Ubuntu;

7.1.1.2. Red Hat® Enterprise Linux®;

7.1.1.3. CentOS;

7.1.1.4. Debian GNU / Linux.

7.1.2. Plataforma 64-bits:

7.1.2.1. Ubuntu;

7.1.2.2. Red Hat Enterprise Linux;

7.1.2.3. CentOS;

7.1.2.4. Debian GNU / Linux;

7.1.2.5. OracleLinux;

7.1.2.6. SUSE® Linux Enterprise Server;

7.1.2.7. openSUSE®.

7.2. Características:

7.2.1. Deve prover as seguintes proteções:

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

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

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

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

7.2.6. 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;

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

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

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

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

7.2.11. 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;

7.2.12. Capacidade de verificar objetos usando heurística;

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

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

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

8. SMARTPHONES E TABLETS

8.1. Compatibilidade:

8.1.1. Dispositivos com os sistemas operacionais:

8.1.2. Android;

8.1.3. Apple iOS;

8.2. Características:

8.2.1. Deve prover as seguintes proteções:

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

8.2.3. Proteção contra adware e autodialers;

8.2.4. 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;

8.2.5. Arquivos abertos no smartphone;

8.2.6. Programas instalados usando a interface do smartphone;

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

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

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

8.2.10. Deverá bloquear spams de SMS através de Blacklists;

8.2.11. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;

8.2.12. Capacidade de desativar por política:

8.2.12.1. Wi-fi;

8.2.12.2. Câmera;

8.2.12.3. Bluetooth.

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

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

8.2.15. Deverá ter firewall pessoal (Android);

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

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

8.2.18. Capacidade de enviar comandos remotamente de:

8.2.18.1. Localizar;

8.2.18.2. Bloquear.

8.2.19. Capacidade de detectar Jailbreak em dispositivos iOS;

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

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

8.2.22. Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído;

8.2.23. Capacidade de configurar White e black list de aplicativos;

8.2.24. Capacidade de localizar o dispositivo quando necessário;

8.2.25. Permitir atualização das definições quando estiver em "roaming";

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

8.2.27. Deve permitir verificar somente arquivos executáveis;

8.2.28. Deve ter a capacidade de desinfectar o arquivo se possível;

8.2.29. Capacidade de agendar uma verificação;

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

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

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

8.2.32.1. Deletar;

8.2.32.2. Ignorar;

8.2.32.3. Quarentenar;

8.2.32.4. Perguntar ao usuário.

9. GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM)

9.1. Compatibilidade:

9.1.1. Dispositivos com os sistemas operacionais:

9.1.2. Android;

9.1.3. Apple iOS;

9.1.4. Windows Phone.

9.2. Características:

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

9.2.2. Capacidade de ajustar as configurações de:

9.2.3. Sincronização de e-mail;

9.2.4. Uso de aplicativos;

9.2.5. Senha do usuário;

9.2.6. Criptografia de dados;

9.2.7. Conexão de mídia removível.

9.2.8. Capacidade de instalar certificados digitais em dispositivos móveis;

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

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

9.2.11. Capacidade de, remotamente, bloquear um dispositivo iOS;

9.2.12. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;

9.2.13. Permitir sincronização com perfil do “Touch Down”;

9.2.14. Capacidade de desinstalar remotamente o antivírus do dispositivo;

9.2.15. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;

9.2.16. Capacidade de sincronizar com Samsung Knox;

9.2.17. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

10. CRIPTOGRAFIA

10.1. Compatibilidade

10.1.1. Microsoft Windows 7 Professional/Enterprise/Ultimate;

10.1.2. Microsoft Windows 8 Professional/Enterprise;

10.1.3. Microsoft Windows 8.1 Professional/Enterprise;

10.1.4. Microsoft Windows 10 Professional/Enterprise;

10.1.5. Microsoft Windows 11 Professional/Enterprise.

10.2. Características

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

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

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

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

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

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

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

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

10.2.9. Criptografar todos os arquivos individualmente;

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

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

10.2.12. 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;

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

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

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

10.2.16. Possibilita estabelecer parâmetros para a senha de criptografia;

10.2.17. Bloqueia o reuso de senhas;

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

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

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

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

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

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

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

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

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

10.2.27. Capacidade de deletar arquivos de forma segura após a criptografia;

10.2.28. Capacidade de criptografar somente o espaço em disco utilizado;

10.2.29. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

10.2.30. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

10.2.31. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;

10.2.32. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

10.2.33. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

10.2.34. Capacidade de fazer “Hardware encryption”;

11. GERENCIAMENTO DE SISTEMAS

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

11.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

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

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

11.5. Capacidade de gerenciar licenças de softwares de terceiros;

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

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

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

11.9. Suporta modo de instalação silenciosa;

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

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

11.12. Utiliza tecnologia multicast para evitar tráfego na rede;

11.13. Possibilita criar um inventário centralizado de imagens;

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

11.15. Suporte a WakeOnLan para deploy de imagens;

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

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

11.18. Capacidade de gerar relatórios de vulnerabilidades e patches;

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

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

11.21. Permite baixar atualizações para o computador sem efetuar a instalação;

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

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

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

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

11.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

11.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

11.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;

11.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;

11.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.

ITEM 2 - KASPERSKY HYBRID CLOUD SECURITY CPU STANDARD (PLUS)

12. REQUISITOS GERAIS

12.1. Todas as licenças fornecidas terão validade de 36 (trinta e seis) meses para atualizações inerentes ao produto;

12.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus, quanto do software;

12.3. As atualizações deverão ser disponibilizadas através de site na Internet, ou através do próprio software;

12.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para a CONTRATADA além daquele já cotado na proposta;

12.5. As licenças deverão ser associadas a quantidade de CPUs (Sockets) utilizado no ambiente de virtualização do TCE/RN, dessa forma o licenciamento não poderá limitar por quantidade de máquinas virtuais (VMs) do ambiente.

12.6. O serviço de implantação e treinamento *hand's on* deverá estar incluso no fornecimento das licenças.

13. REQUISITOS PARA GERENCIAMENTO, ADMINISTRAÇÃO E RELATÓRIOS CENTRALIZADOS

13.1. A solução proposta deve permitir a instalação de software anti-malware a partir de um único pacote de distribuição.

13.2. A solução proposta deve ter perfis de instalação personalizáveis dependendo do número de nós protegidos.

13.3. A solução proposta deve suportar endereços IPv6.

13.4. A solução proposta deve suportar verificação em duas etapas (autenticação).

13.5. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

13.6. A solução proposta deverá incluir uma consola web incorporada para a gestão dos endpoints, que não deverá necessitar de qualquer instalação adicional.

13.7. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos de tela sensível ao toque.

13.8. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento se novos computadores aparecerem na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.

13.9. A solução proposta deverá prever a instalação, atualização e remoção centralizada de software anti-malware, bem como configuração, administração e visualização centralizada de relatórios e informações estatísticas sobre o seu funcionamento.

13.10. A solução proposta deve contemplar a remoção centralizada (manual e automática) de aplicativos incompatíveis do centro de administração.

13.11. A solução proposta deve fornecer métodos flexíveis para a instalação do agente antimalware: RPC, GPO, um agente de administração para instalação remota e a opção de criar um pacote de instalação autônomo para instalação local.

13.12. A solução proposta deve permitir a instalação remota de software anti-malware com as bases de dados anti-malware mais recentes.

13.13. A solução proposta deve permitir a atualização automática do software antimalware e das bases de dados antimalware.

13.14. A solução proposta deve possibilitar o gerenciamento de um componente que proíba a instalação e/ou execução de programas.

13.15. A solução proposta deve possibilitar o gerenciamento de um componente controlando o trabalho com dispositivos de E/S externos.

13.16. A solução proposta deve possibilitar o gerenciamento de um componente que controla a atividade do usuário na internet.

13.17. A solução proposta deve permitir o teste das atualizações baixadas por meio do software de administração centralizada antes de distribuí-las às máquinas clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.

13.18. A solução deve ter a capacidade de executar uma implantação automática com base na solicitação do sistema de proteção dedicado para infraestruturas virtuais baseadas na virtualização VMware ESXi , Microsoft Hyper-V, Citrix XenServer , HUAWEI FusionSphere , KVM, Nutanix Acropolis, Skala-R, Proxmox VE plataforma ou hipervisor.

13.19. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração em um nível arbitrário e a capacidade de gerenciar centralmente toda a hierarquia a partir do nível superior.

13.20. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidor de administração logicamente isoladas possam ser configuradas para diferentes usuários e grupos de usuários.

13.21. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

13.22. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

13.23. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software anti-malware instalado e nas configurações, e para distribuir notificações sobre eventos via e-mail.

13.24. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em alguns computadores.

13.25. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como um centro para retransmitir atualizações e pacotes de

instalação, a fim de reduzir a carga de rede no sistema principal do servidor de administração.

13.26. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como um centro de encaminhamento de eventos do agente anti-malware do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga de rede no sistema principal do servidor de administração .

13.27. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware, e dados sobre o inventário de hardware e software, licenciamento, etc.

13.28. A solução proposta deve ser capaz de exportar relatórios para arquivos PDF e XML.

13.29. A solução proposta deve fornecer a administração centralizada de armazenamentos de backup e quarentena em todos os recursos de rede onde o software anti-malware está instalado.

13.30. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

13.31. A solução proposta deve prever a criação de uma cópia de backup do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.

13.32. A solução proposta deve oferecer suporte ao Windows Failover Cluster.

13.33. A solução proposta deve ter um recurso de cluster integrado.

13.34. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.

13.35. A solução proposta deve incluir Controle de Acesso Baseado em Função (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

13.36. O servidor de gerenciamento da solução proposta deve incluir funções de segurança pré-definidas para Auditor, Supervisor e Agente de Segurança.

13.37. A solução proposta deve ter capacidade de gerenciar dispositivos móveis por meio de comandos remotos.

13.38. A solução proposta deve ter a capacidade de excluir as atualizações baixadas.

13.39. A solução proposta deve gerar atualizações do Servidor de Administração de Gerenciamento a partir da interface do aplicativo.

13.40. A solução proposta deve permitir a seleção de um agente de atualização para computadores clientes com base em uma análise de rede.

13.41. O servidor de gerenciamento da solução proposta deve manter um histórico de revisão das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que as modificações em uma determinada política/tarefa possam ser revisadas.

13.42. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar vários perfis dentro de uma política de proteção com diferentes configurações de proteção que podem ser ativadas simultaneamente em um único/vários dispositivos com base nas seguintes regras de ativação:

13.42.1. Status do dispositivo

13.42.2. Tag

13.42.3. Diretório ativo

13.42.4. Proprietários de dispositivos

13.43. hardware

13.44. A solução proposta deve suportar os seguintes canais de entrega de notificação:

13.44.1. E-mail

13.44.2. Syslog

13.45. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.

13.46. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos . arquivos dll .

13.47. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

13.47.1. Atributos de rede

13.47.2. Nome

13.47.3. Domínio e/ou Sufixo de Domínio

13.47.4. endereço de IP

13.47.5. Endereço IP para o servidor de gerenciamento

13.47.6. Localização no Active Directory

13.47.7. Unidade organizacional

13.47.8. Grupo

13.47.9. Sistema operacional

13.47.10. Tipo e versão

13.47.11. Arquitetura

13.47.12. Número do pacote de serviço

13.47.13. Arquitetura virtual

13.47.14. Registro de aplicativos

13.47.15. Nome da Aplicação

13.47.16. Versão do aplicativo

13.47.17. Fabricante

13.48. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gerenciamento.

13.49. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectando pela internet/rede pública.

13.50. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

13.51. A solução proposta deve ter um painel personalizável gerando e exibindo estatísticas em tempo real para endpoints.

13.52. A solução proposta deve permitir que o administrador personalize os relatórios.

13.53. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.

13.54. A solução proposta deve permitir que o administrador estabeleça um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados são excluídos automaticamente do servidor.

13.55. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

13.55.1. Nome da Aplicação

13.55.2. Caminho do Aplicativo

13.55.3. Metadados do aplicativo

13.55.4. Aplicativo certificado digital

13.55.5. Categorias de aplicativos pré-definidas pelo fornecedor

13.55.6. SHA

13.56. Computadores de referência para permitir/negar sua execução em endpoints.

13.57. A solução proposta deve permitir que o administrador defina diferentes condições de alteração de status para grupos de endpoints no servidor de gerenciamento.

13.58. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

13.59. A solução proposta deve ter um recurso/módulo embutido para coletar remotamente os dados necessários para solução de problemas dos endpoints, sem exigir acesso físico.

13.60. A solução proposta deve permitir que o administrador crie um Túnel de Conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta utilizada para conexão com o servidor de gerenciamento não esteja disponível no dispositivo.

13.61. A solução deve ter funcionalidade integrada para se conectar remotamente ao ponto de extremidade usando a tecnologia de compartilhamento de área de trabalho do Windows. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

13.62. A solução proposta deve possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

13.62.1. estruturas de domínios e grupos de trabalho do Windows

13.62.2. estruturas de grupos do Active Directory

13.62.3. conteúdo de um arquivo de texto criado pelo administrador manualmente

13.63. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa de rede. O inventário resultante deve abranger todos os equipamentos conectados à rede da organização.

13.64. As informações sobre o equipamento devem ser atualizadas após cada nova pesquisa de rede. A lista de equipamentos detectados deve abranger o seguinte:

13.64.1. dispositivos

13.64.2. dispositivos móveis

13.64.3. dispositivos de rede

13.64.4. dispositivos virtuais

13.64.5. componentes OEM

13.64.6. periféricos de computador

13.64.7. dispositivos conectados

13.64.8. telefones VoIP

13.64.9. repositórios de rede

13.65. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

13.66. A funcionalidade 'Device is Write Off' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

13.67. A solução proposta deve incorporar um único agente de distribuição/retransmissão para retransmitir/transferir ou fazer proxy de solicitações de reputação de ameaças de endpoints para o servidor de gerenciamento.

13.68. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

13.69. A solução proposta deve suportar OPEN API e incluir diretrizes para integração com sistemas externos de terceiros.

13.70. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem a necessidade de acesso físico ao computador.

13.71. A solução proposta deve incluir Controle de Acesso Baseado em Função (RBAC) com funções predefinidas personalizáveis.

13.72. O servidor de gerenciamento primário/pai da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

13.73. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

13.74. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados nos dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos.

13.75. O servidor de gerenciamento principal da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundário.

13.76. A solução proposta deve incluir a opção para o cliente implantar um console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

13.77. A solução proposta deve incluir as seguintes opções de integração SIEM:

13.77.1. Syslog

13.78. A solução proposta deve fornecer mecanismos de atualização de banco de dados anti-malware, incluindo:

13.78.1. Múltiplas formas de atualização, incluindo canais de comunicação globais sobre o protocolo HTTPS, recurso compartilhado na rede local e mídia removível.

13.78.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

14. REQUISITOS DO MÓDULO DE PROTEÇÃO BASEADA EM AGENTE PARA SISTEMA OPERACIONAIS WINDOWS

14.1. A solução deve oferecer suporte aos seguintes sistemas operacionais Windows:

14.2. Sistemas operacionais Microsoft Windows de 32 bits:

14.2.1. Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou posterior

14.2.2. Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter SP2 ou posterior

14.2.3. Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou posterior

14.2.4. Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 ou posterior

14.2.5. Sistemas operacionais Microsoft Windows de 64 bits:

14.2.6. Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou posterior

14.2.7. Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou posterior

14.2.8. Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 ou posterior

14.2.9. Windows Server 2008 Standard / Premium SP1 ou posterior

14.2.10. Microsoft Small Business Server 2008 Standard/Premium

14.2.11. Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 ou posterior

14.2.12. Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 ou posterior

14.2.13. Windows Hyper-V Server 2008 R2 SP1 ou posterior

14.2.14. Microsoft Small Business Server 2011 Essentials / Standard

14.2.15. Microsoft Windows MultiPoint Server 2011 Standard/Premium

14.2.16. Windows Server 2012 Foundation / Essentials / Standard / Datacenter

14.2.17. Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter

14.2.18. Microsoft Windows MultiPoint Server 2012 Standard/Premium

14.2.19. Servidor de armazenamento do Windows 2012

14.2.20. Windows Hyper-V Server 2012

14.2.21. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter

14.2.22. Windows Server 2012 R2 Core / Foundation / Essentials / Standard / Datacenter

14.2.23. Servidor de armazenamento do Windows 2012 R2

14.2.24. Windows Hyper-V Server 2012 R2

14.2.25. Windows Server 2016 Essentials / Standard / Datacenter

14.2.26. Windows Server 2016 MultiPoint

14.2.27. Windows Server 2016 Core Standard / Datacenter

14.2.28. Microsoft Windows MultiPoint Server 2016

14.2.29. Servidor de armazenamento do Windows 2016

14.2.30. Windows Hyper-V Server 2016

14.2.31. Windows Server 2019 Essentials / Standard / Datacenter

14.2.32. Windows Server Core 2019

14.2.33. Servidor de armazenamento do Windows 2019

14.2.34. Windows Hyper-V Server 2019

14.3. Servidores de terminal:

14.3.1. Terminal Server Windows Server 2008

14.3.2. Terminal Server Windows Server 2008 R2

14.3.3. Terminal Server Windows Server 2012

14.3.4. Terminal Server Windows Server 2012 R2

14.3.5. Terminal Server Windows Server 2016

14.3.6. Terminal Server Windows Server 2019

14.3.7. Terminal Server Windows Server 2022

14.4. Requisitos funcionais

14.4.1. A solução deve oferecer suporte à verificação de objetos quando eles são acessados.

14.4.2. A solução deve oferecer suporte a verificações dos seguintes objetos:

14.4.2.1. arquivos

14.4.2.2. Fluxos alternativos do sistema de arquivos (fluxos NTFS)

14.4.3. Registro de inicialização e setores de inicialização em discos rígidos locais e unidades removíveis;

14.5. A solução deve suportar varredura sob demanda para execute uma única verificação da área especificada em busca de vírus e outras ameaças à segurança do computador. A solução verifica arquivos, RAM e objetos de inicialização em um dispositivo protegido.

14.6. A solução deve oferecer suporte ao controle de dispositivos para controlar o registro e o uso de dispositivos externos, a fim de proteger o dispositivo contra ameaças de segurança que possam surgir durante a troca de arquivos com unidades flash conectadas por USB ou outros tipos de dispositivos externos.

14.7. A solução deve oferecer suporte a pastas compartilhadas de proteção em dispositivos contra criptografia maliciosa, bloqueando hosts que mostram atividade maliciosa.

14.8. A solução deve controlar a execução de scripts usando tecnologias de script do Microsoft Windows.

14.9. A solução deve oferecer suporte à interceptação e verificação de objetos transferidos por meio do tráfego da Web (incluindo e-mail) para detectar computadores conhecidos e outras ameaças no dispositivo protegido.

14.10. A solução deve verificar o tráfego de rede em busca de atividades típicas de ataques de rede e bloquear a atividade de rede do computador atacante.

14.11. A solução deve fornecer ao administrador a capacidade de gerenciar o Firewall do Windows: definir as configurações e as regras de firewall do sistema operacional e bloquear qualquer tentativa externa de configurar o firewall.

14.12. A solução deve fornecer ao administrador a capacidade de atualizar a solução para servidores de atualização FTP ou HTTP na Internet, a partir do sistema de gerenciamento central ou outras fontes de atualização.

14.13. A solução deve colocar em quarentena os objetos provavelmente infectados, movendo-os de seu local original para a pasta de quarentena. Por motivos de segurança, os objetos na pasta de quarentena devem ser armazenados de forma criptografada

14.14. A solução deve armazenar cópias criptografadas de objetos classificados como infectados no backup antes de desinfetá-los ou excluí-los.

14.15. A solução deve oferecer suporte a notificações do usuário.

14.16. A solução deve oferecer suporte à importação e exportação de configurações.

14.17. A solução deve permitir que o administrador gere uma lista de exclusões do escopo de proteção ou verificação, que a solução aplicará na verificação sob demanda e em tempo real.

14.18. A solução deve oferecer suporte à proteção de memória contra explorações.

15. REQUISITOS DO MÓDULO DE PROTEÇÃO BASEADA EM AGENTE PARA SISTEMAS OPERACIONAIS LINUX

15.1. A solução deve oferecer suporte aos seguintes sistemas operacionais Linux:

15.2. Sistemas operacionais de 32 bits:

15.2.1. CentOS 6.7 e posterior.

15.2.2. Debian GNU/Linux 10.1 e posterior.

15.2.3. Debian GNU/Linux 11.

15.2.4. Red Hat Enterprise Linux 6.7 e posterior.

15.2.5. Desktop ALT 8 SP.

15.2.6. Server ALT 8SP.

15.2.7. ALT Education 10.

15.2.8. Desktop ALT 10.

15.3. Sistemas operacionais de 64 bits:

15.3.1. AlmaLinux OS 8 e posterior.

15.3.2. AlmaLinux OS 9 e posterior.

15.3.3. AlterOS 7.5 e posterior.

15.3.4. AmazonLinux 2.

15.3.5. Astra Linux.

15.3.6. CentOS 6.7 e posterior.

15.3.7. CentOS 7.2 e posterior.

15.3.8. CentOS Fluxo 9.

15.3.9. Debian GNU/Linux 10.1 e posterior.

15.3.10. Debian GNU/Linux 11.

15.3.11. Linux Mint 19.2 e posterior.

15.3.12. Linux Mint 20.3 e posterior.

15.3.13. openSUSE Leap 15.0 e posterior.

15.3.14. Oracle Linux 7.3 e posterior.

15.3.15. Oracle Linux 8.0 e posterior.

15.3.16. Red Hat Enterprise Linux 6.7 e posterior.

15.3.17. Red Hat Enterprise Linux 7.2 e posterior.

15.3.18. Red Hat Enterprise Linux 8.0 e posterior.

15.3.19. RedHat Enterprise Linux 9.

15.3.20. Rocky Linux 8.5 e posterior.

15.3.21. SUSE Linux Enterprise Server 12.5 ou posterior.

15.3.22. SUSE Linux Enterprise Server 15 ou posterior.

15.3.23. Ubuntu 20.04LTS.

15.3.24. Ubuntu 22.04LTS.

15.3.25. Desktop ALT 8 SP.

15.3.26. Server ALT 8SP.

15.3.27. Desktop ALT 10.

15.3.28. Server ALT 10.

15.4. Sistemas operacionais de 64 bits para a arquitetura ARM:

15.4.1. Astra Linux Special Edition RUSB.10152-02 (atualização operacional 4.7).

15.4.2. SUSE Linux Enterprise Server 15 SP3.

15.4.3. Ubuntu 20.04LTS.

15.4.4. Servidor ALT 8SP.

15.5. Requisitos funcionais

15.6. A solução deve oferecer suporte a objetos do sistema de arquivos de varredura localizados nas unidades locais do computador, bem como recursos montados e compartilhados acessados por meio dos protocolos SMB e NFS.

15.7. A solução deve oferecer suporte a varredura de objetos do sistema de arquivos em tempo real e sob demanda.

15.8. A solução deve oferecer suporte a digitalização de objetos de inicialização , setores de inicialização, processo e memória do kernel

15.9. A solução deve suportar neutralizar ameaças detectadas em arquivos e escolher automaticamente qual ação executar para neutralizar a ameaça

15.10. A solução deve oferecer suporte ao armazenamento de cópias de backup de arquivos antes da desinfecção ou exclusão e restauração de arquivos de cópias de backup

15.11. A solução deve oferecer suporte à notificação do administrador sobre eventos ocorridos durante a operação

15.12. A solução deve oferecer suporte à atualização de bancos de dados dos servidores na Internet, por meio do servidor de gerenciamento central ou de uma fonte especificada pelo administrador por agendamento ou sob demanda.

15.13. A solução deve oferecer suporte à adição de chaves, bem como à ativação usando códigos de ativação.

15.14. A solução deve oferecer suporte ao gerenciamento de um firewall do sistema operacional.

15.15. A solução deve oferecer suporte à proteção de seus arquivos nos diretórios locais com acesso à rede por protocolos SMB/NFS contra criptografia maliciosa remota.

15.16. A solução deve oferecer suporte à verificação de tráfego por meio dos protocolos HTTP/HTTPS e FTP e verificar se os endereços da Web são maliciosos ou phishing.

15.17. A solução deve oferecer suporte ao controle de dispositivo configurável para restringir o acesso do usuário aos dispositivos (como discos rígidos, unidades removíveis, CDs, DVDs, modems, impressoras, USB, FireWire). O controle do dispositivo deve ser capaz de operar no modo somente notificação.

15.18. A solução deve oferecer suporte ao gerenciamento de dispositivos conectados com limitações de tempo e usuário por meio do Samba Active Directory e do Microsoft Active Directory.

15.19. A solução deve oferecer suporte à verificação de unidades removíveis quando elas estão conectadas a um computador.

15.20. A solução deve oferecer suporte à inspeção de tráfego de rede para atividades típicas de ataques de rede. Deve ser capaz de operar no modo somente notificação.

15.21. A solução deve suportar a verificação da reputação do objeto no banco de dados de reputação global.

15.22. A solução deve permitir que usuários não root gerenciem as funções básicas do aplicativo usando a GUI.

15.23. A solução deve oferecer suporte ao gerenciamento usando os seguintes métodos:

15.23.1. Na linha de comando usando os comandos de controle de aplicativos.

15.23.2. Via console de gerenciamento central (console baseado em MMC e console da web).

15.23.3. Usando GUI local.

15.24. A solução deve suportar capacidade de detecção de comportamento. Deve ser capaz de operar no modo somente notificação.

15.25. A solução deve suportar o trabalho com o sistema de arquivos GlusterFS .

15.26. A solução deve suportar verificação da memória do kernel

15.27. A solução deve oferecer suporte à verificação da integridade dos componentes do aplicativo.

15.28. A solução deve oferecer suporte aos recursos de controle de inicialização do aplicativo.

15.29. A solução deve ser capaz de obter informações sobre todos os arquivos de programas executáveis armazenados nos computadores.

15.30. A solução deve oferecer suporte à opção de gerenciamento baseado em perfil.

16. REQUISITOS DO MÓDULO PARA SOLUÇÃO DE ANTIMALWARE BASEADO EM AGENTES PARA DATACENTER:

16.1. A solução deve suportar a seguinte infraestrutura virtual:

16.1.1. Plataforma Microsoft Hyper-V:

16.1.2. Hipervisor Microsoft Windows Server 2019 Hyper-V (no modo completo ou no modo Server Core)

16.1.3. Microsoft Windows Server 2016 Hyper-V hypervisor (no modo completo ou no modo Server Core) com todas as atualizações disponíveis

16.1.4. Microsoft Windows Server 2012 R2 Hyper-V hypervisor (no modo completo ou no modo Server Core) com todas as atualizações disponíveis

16.2. Plataforma Citrix Hypervisor:

16.2.1. Citrix 8.2 LTSR .

16.3. Plataforma VMware vSphere:

16.3.1. Hypervisor VMware ESXi 7.0 com as atualizações mais recentes

16.3.2. Hypervisor VMware ESXi 6.7 com as atualizações mais recentes

16.3.3. Hypervisor VMware ESXi 6.5 com as atualizações mais recentes

16.4. Ao proteger máquinas virtuais na infraestrutura VMware, o Kaspersky Security pode usar um dos seguintes tipos de VMware NSX Manager:

16.4.1. VMware NSX-V Manager do pacote VMware NSX Data Center para vSphere 6.4.6.

16.4.2. VMware NSX-T Manager do pacote VMware NSX-T Data Center 2.5.1.

16.4.3. VMware NSX-T Manager do pacote VMware NSX-T Data Center 3.0.0.

16.5. Plataforma KVM: hypervisor KVM com um dos seguintes sistemas operacionais:

16.5.1. Servidor Ubuntu 20.04 LTS

16.5.2. Servidor Ubuntu 18.04 LTS

16.5.3. Servidor Ubuntu 16.04 LTS

16.5.4. Servidor Red Hat Enterprise Linux 7. 9

16.5.5. CentOS 7.9

16.6. Proxmox VE:

16.6.1. Proxmox VE 6.4

16.6.2. Proxmox VE 6.3

16.7. Plataforma Skala-R:

16.7.1. Hipervisor R-Virtualization 7.0.13.

16.7.2. HUAWEI FusionSphere :

16.7.3. HUAWEI FusionCompute CNA 8.0.

16.8. Plataforma Nutanix Acrópole:

16.8.1. Hipervisor Nutanix AHV 5.19.1.

16.9. Plataforma SharxBase :

16.9.1. Hipervisor SharxBase 5.10.x

16.10. Plataforma OpenStack:

16.10.1. Lançamentos da plataforma OpenStack: Stein, Victoria, Wallaby ou Xena

16.11. A solução deve suportar as seguintes soluções de virtualização:

16.11.1. Citrix Virtual Apps and Desktops 7 1912 LTSR.

16.11.2. Citrix XenApp e XenDesktop 7.15 LTSR.

16.11.3. Provisionamento Citrix 7 1912 LTSR.

16.11.4. Serviços de Provisionamento Citrix 7.15 LTSR.

16.11.5. VMware Horizon 8.2 (2103).

16.11.6. Volumes de aplicativos VMware (2103).

16.11.7. HUAWEI FusionAccess 8.0 e posterior.

16.12. A solução deve oferecer suporte aos seguintes sistemas operacionais Windows:

16.12.1. Windows 11 21H2 Pro/Enterprise/Educação

16.12.2. Windows 10 Desktop Pro / Enterprise / 2016 LTSC / RS4 / 2019 LTSC / 19H1 / 19H2 / 20H1 (32 / 64 bits)

16.12.3. Windows 8.1 Update 1 Professional/Enterprise (32/64 bits)

16.12.4. Windows 7 Professional / Enterprise Service Pack 1 (32/64 bits)

16.12.5. Windows Server 2019 Standard/ Datacenter (64 bits)

16.12.6. Windows Server 2016 Standard/ Datacenter (64 bits)

16.13. Windows Server 2012 R2 Standard / Datacenter / Essentials (64 bits)

16.13.1. Windows Server 2012 Standard / Datacenter / Essentials (64 bits)

16.13.2. Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter (64 bits)

16.14. A solução deve oferecer suporte aos seguintes sistemas operacionais Linux:

16.14.1. Debian GNU/Linux 10.3 (32/64 bits)

16.14.2. Debian GNU/Linux 9.8 (64 bits)

16.14.3. Debian GNU/Linux 8.11 (64 bits)

16.14.4. Debian GNU/Linux 8.11 i386 (32 bits)

16.14.5. Ubuntu Server 20.04 LTS (64 bits)

16.14.6. Servidor Ubuntu 18.04 LTS (64 bits)

16.14.7. Servidor Ubuntu 16.04 LTS (64 bits)

16.14.8. CentOS 8.1 (64 bits)

16.14.9. CentOS 7.7 (64 bits)

16.14.10. CentOS 6.10 (64 bits)

16.14.11. Red Hat Enterprise Linux Server 8.1 (64 bits)

16.14.12. Red Hat Enterprise Linux Server 7.7 (64 bits)

16.14.13. Red Hat Enterprise Linux Server 6.10 (64 bits)

16.14.14. SUSE Linux Enterprise Server 15 (64 bits)

16.14.15. ALT Linux 8 (64 bits)

16.14.16. ALT Linux 7.0.6 (64 bits)

16.14.17. Oracle Linux 7.6 (64 bits)

16.14.18. AstraLinux SE 1.6

16.14.19. AstraLinux SE 1.5

16.15. Requisitos funcionais

16.16. A solução deve oferecer suporte ao monitoramento antimalware residencial.

16.17. A solução deve ter um analisador heurístico para detectar e bloquear malware anteriormente desconhecido.

16.18. A solução deve executar a verificação antimalware e outras tarefas com uso intensivo de recursos em uma máquina virtual segura dedicada, e não em máquinas virtuais convidadas.

16.19. Se a máquina virtual segura principal estiver indisponível, o Light Agent deve oferecer suporte à detecção automática e reconexão a uma máquina virtual segura em funcionamento, incluindo uma que esteja operando em um host diferente.

16.20. Técnicas de redundância, que permitem a reconexão do Light Agent a qualquer máquina virtual segura dentro da infraestrutura sem qualquer (re)configuração manual.

16.21. A solução deve oferecer suporte à instalação remota do Light Agent para Windows e Linux.

16.22. A solução deve garantir a continuidade da proteção de arquivo durante a indisponibilidade de curto prazo da máquina virtual segura, registrando todas as operações de arquivo durante o período de indisponibilidade e verificação automática de todas as alterações após a restauração do acesso.

16.23. A solução deve oferecer suporte à proteção baseada em nuvem contra novas ameaças, permitindo que o aplicativo acesse um banco de dados de reputação global para obter veredictos de arquivos durante a verificação em tempo real ou programada.

16.24. A solução deve oferecer suporte à proteção de e-mails contra malware, verificando o tráfego de entrada e saída nos protocolos IMAP, SMTP, POP3, NNTP, independentemente do cliente de e-mail, tanto em servidores quanto em estações de trabalho.

16.25. A solução deve oferecer suporte à proteção do tráfego da Web: verificação de objetos – incluindo o uso de análise heurística – via protocolos HTTP, FTP, HTTPS, FTPS, WS ou WSS e analisa essas páginas ou arquivos da Web quanto à presença de vírus ou outro malware , com a capacidade de configurar sites confiáveis.

16.26. A solução deve oferecer suporte à verificação do tráfego da Web de entrada e saída de uma máquina virtual protegida e verifica os endereços da Web nos bancos de dados de endereços da Web maliciosos e de phishing (sites da Web), bem como o bloqueio desses sites.

16.27. A solução deve oferecer suporte à proteção contra programas maliciosos ainda desconhecidos com base em seu comportamento.

16.28. A solução deve oferecer suporte à capacidade de determinar o comportamento anômalo de um aplicativo analisando sua sequência de execução. Capacidade de reverter operações de malware durante o tratamento.

16.29. A solução deve oferecer suporte à capacidade de restringir os privilégios de programas executáveis, como gravar no registro ou acessar arquivos e pastas. Detecção automática de níveis de restrição com base na reputação do programa.

16.30. A solução deve fornecer os recursos para programas de terceiros enviarem solicitações de verificação de objetos em busca de vírus e outras ameaças usando a interface de verificação antimalware do Windows (AMSI).

16.31. A solução deve oferecer suporte ao firewall integrado que permite que regras de pacotes de rede sejam definidas para protocolos e portas específicos (TCP, UDP). Criação de regras de rede para programas específicos.

16.32. Componente que permite a criação de regras especiais para bloquear a instalação e/ou execução de um programa. O componente deve ser capaz de controlar o aplicativo por meio do caminho do programa, metadados, soma de verificação MD5 e categorias predefinidas de aplicativos fornecidos pelo fornecedor. Ele também deve permitir exceções às regras para usuários específicos do AD.

16.33. Monitoramento da atividade do usuário com dispositivos de E/S externos por tipo de dispositivo e/ou barramento, incluindo a capacidade de criar uma lista de dispositivos confiáveis por seu ID e a capacidade de conceder privilégios para usar dispositivos externos a usuários AD específicos.

16.34. A solução deve armazenar as atualizações do banco de dados antimalware em máquinas virtuais seguras.

16.35. A solução deve permitir que os administradores instalem e distribuam remotamente componentes de software antimalware em todas as máquinas virtuais protegidas sem usar ferramentas de terceiros.

16.36. A solução deve oferecer suporte à verificação programada de todas as máquinas virtuais.

16.37. A solução deve ter um único console de gerenciamento para todos os componentes de proteção.

16.38. A solução deve ter um único console de gerenciamento centralizado para ambientes virtuais e estações de trabalho físicas.

16.39. A solução deve oferecer suporte ao controle de dispositivos para restringir o acesso a dispositivos que são fontes de informações (por exemplo, discos rígidos, unidades removíveis, discos de CD/DVD, modems, impressoras, USB ou Bluetooth.

16.40. A solução deve oferecer suporte ao controle da Web de controle de dispositivo para restringir o acesso do usuário aos recursos da Web. A solução deve permitir a implementação de intervalos de tempo para controle e a capacidade de atribuí-los apenas a usuários específicos do AD.

16.41. A solução deve oferecer suporte ao controle de privilégio do aplicativo que registra a atividade dos aplicativos no sistema operacional da máquina virtual protegida e regula a atividade do aplicativo, dependendo do grupo ao qual o aplicativo foi atribuído.

16.42. A solução deve fornecer informações detalhadas sobre eventos em máquinas virtuais e execução de tarefas de proteção.

16.43. A solução deve oferecer suporte à verificação de mensagens de e-mail recebidas e enviadas em busca de vírus e outros malwares.

16.44. A solução deve permitir que os administradores apliquem diferentes configurações de segurança para diferentes grupos de máquinas virtuais.

16.45. A solução deve oferecer suporte ao armazenamento de cópias de backup de arquivos excluídos.

16.46. A solução deve suportar a tecnologia VMware: vMotion , DRS

16.47. A solução deve oferecer suporte para reversão de bancos de dados de antivírus.

16.48. A solução deve suportar um esquema de licenciamento de acordo com o número de máquinas virtuais protegidas e de acordo com o número de núcleos de CPU de hardware.

16.49. A solução deve oferecer suporte à proteção de máquinas virtuais que executam os sistemas operacionais Windows e Linux.

16.50. A solução deve oferecer suporte ao console de administração unificado para implantação e gerenciamento eficientes de toda a infraestrutura de segurança de TI.

16.51. A solução deve oferecer suporte à prevenção automática de exploração que pode bloquear a exploração de vulnerabilidades de aplicativos comumente usadas por criminosos cibernéticos, aumentando drasticamente o nível geral de proteção.

16.52. A solução deve oferecer suporte a recursos que monitoram o comportamento de aplicativos em execução e regulam suas atividades, incluindo proteção contra ameaças baseada em comportamento para VMs convidadas do Windows Server.

16.53. A solução deve ter proteção de rede integrada, que detecta e bloqueia ataques diretos à rede.

16.54. A solução deve oferecer suporte à proteção da Web integrada, que detecta e bloqueia URLs maliciosos.

16.55. Verifica todos os arquivos durante a verificação antimalware (mesmo arquivos maiores que 30 Mb).

16.56. A solução deve suportar o envio de notificações por e-mail e SMS

16.57. A solução deve ter uma política de segurança para gerenciar todos os módulos de proteção.

16.58. A solução deve ser compatível com NSX Security Tags

16.59. A solução deve oferecer suporte à proteção de pastas compartilhadas contra criptografia remota

16.60. A solução deve oferecer suporte para ativação usando um código de ativação fornecido na assinatura.

16.61. A solução deve oferecer suporte à verificação de conexões seguras estabelecidas usando os protocolos SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 ou TLS 1.3

16.62. A solução deve ter tarefas de varredura para o Light Agent for Linux, que inclui varredura de setores de inicialização, memória do sistema e objetos de inicialização

16.63. A solução deve oferecer suporte para o sistema de arquivos GlusterFS em máquinas virtuais que tenham o Light Agent for Linux instalado.

16.64. A solução deve permitir o uso do aplicativo no modo multilocação.

16.65. A solução deve fornecer a capacidade de automatizar a implantação e o uso do aplicativo no modo multilocação usando a API REST.

16.66. A solução para o controle obrigatório de aplicativos (negação padrão) para servidores e desktops virtuais que rastreia as tentativas dos usuários de iniciar o aplicativo e controla o início do aplicativo.

16.67. O controle de aplicativos para Windows Servers deve ter lógica de lista branca e lista negra.

16.68. A solução deve fornecer integração com a solução “EDR” de detecção e resposta de endpoint do mesmo fornecedor, para busca ativa de ameaças e automação de resposta a incidentes.

16.69. A solução deve fornecer recursos de integração com o serviço gerenciado de detecção e resposta do mesmo fornecedor.

17. REQUISITOS DO MÓDULO PARA SOLUÇÃO DE ANTIMALWARE SEM AGENTES PARA DATACENTER:

17.1. A solução deve suportar a seguinte infraestrutura virtual:

17.1.1. VMware vSphere versões 8.0 e 7.0

17.1.2. VMware ESXi hipervisor 8.0 ou posterior

17.1.3. VMware ESXi 7.0 Atualização 1c ou posterior

17.1.4. VMware ESXi 6.7 Atualização 3 ou posterior

17.1.5. VMware ESXi 6.5 Atualização 3 ou posterior.

17.1.6. VMware vCenter Servidor 8.0 ou posterior

17.1.7. VMware vCenter Server 7.0 Atualização 1d ou posterior

17.1.8. VMware vCenter Server 6.7 Update 3 ou posterior

17.1.9. VMware vCenter Server 6.5 Atualização 3 ou posterior.

17.2. VMware NSX Manager de um dos seguintes tipos:

17.2.1. NSX-V Manager do pacote VMware NSX Data Center para vSphere 6.4.10.

17.2.2. NSX-T Manager do VMware NSX 4.0.1.1, VMware NSX 4.0.0.1, VMware NSX-T Data Center 3.2.0.1, VMware NSX-T Data Center 3.1.3, VMware NSX-T Data Center 3.1.1 ou VMware NSX -T Data Center 3.0.3 pacote.

17.2.3. VMware NSX-T Manager do pacote VMware NSX 4.0.1.1, VMware NSX 4.0.0.1, VMware NSX-T Data Center 3.2.0.1 ou VMware NSX-T Data Center 3.0.3.

17.2.4. VMware vCloud Director 9.7.0.3 para provedores de serviços

17.2.5. VMware vCloud Diretor versões 10.4, 10.3.3.2, 10.3.2.1, 10.3.0, 10.1.2

17.3. A solução deve oferecer suporte aos seguintes sistemas operacionais Windows:

17.3.1. Windows 11

17.3.2. Windows 10

17.3.3. Windows 8.1

17.3.4. Windows 8

17.3.5. Windows 7 Service Pack 1

17.3.6. WindowsServer 2022

17.3.7. WindowsServer 2019

17.3.8. WindowsServer 2016

17.3.9. Windows Server 2012 R2 sem suporte a ReFS (Resilient File System)

17.3.10. Windows Server 2012 sem suporte a ReFS (Resilient File System)

17.3.11. Windows Server 2008 R2 Service Pack 1

17.4. A solução deve oferecer suporte aos seguintes sistemas operacionais Linux:

17.4.1. Ubuntu Server 18.04 GA (64 bits)

17.4.2. Ubuntu Server 16.04 GA (64 bits)

17.4.3. Ubuntu Server 14.04 GA (64 bits)

17.4.4. Red Hat Enterprise Linux Server 7.7 GA (64 bits)

17.4.5. Red Hat Enterprise Linux Server 7.4 GA (64 bits)

17.4.6. Red Hat Enterprise Linux Server 7.0 GA (64 bits)

17.5. SUSE Linux Enterprise Server 12 GA (64 bits)

17.5.1. CentOS 7.7 GA (64 bits)

17.5.2. CentOS 7.4 GA (64 bits)

17.5.3. CentOS 7.0 GA (64 bits)

17.6. Requisitos funcionais

17.7. A solução deve oferecer suporte à proteção contra malware em tempo real e durante a verificação agendada sem instalar um agente antivírus nas máquinas virtuais convidadas.

17.8. A solução deve oferecer suporte à integração com a tecnologia VMware Network Extensibility SDK para fornecer proteção no nível da rede, implementada para monitorar e suprimir atividades de rede maliciosas, bem como bloquear endereços de URL maliciosos com a capacidade de notificar o usuário sobre o acesso bloqueado.

17.9. A solução deve oferecer suporte à proteção baseada em nuvem contra novas ameaças, permitindo que o aplicativo entre em contato com os recursos especializados do fornecedor de segurança para obter um veredito de arquivo durante a verificação em tempo real ou agendada.

17.10. A solução deve suportar atualizações centralizadas na máquina de proteção especializada sem a necessidade de distribuir atualizações para cada máquina convidada.

17.11. A solução deve oferecer suporte à verificação sob demanda (ou manual) de máquinas virtuais (VM) selecionadas.

17.12. A solução deve oferecer suporte à verificação de arquivos, pastas ou de todo o sistema selecionados.

17.13. A solução deve oferecer suporte à verificação programada de todas as máquinas virtuais.

17.14. A solução deve fornecer a capacidade de implantar uma solução sem reinicialização do hipervisor ou modo de manutenção.

17.15. A solução não deve exigir uma nova verificação dos arquivos.

17.16. A solução deve impedir a nova verificação do mesmo objeto em diferentes máquinas convidadas em um único host.

17.17. A solução deve suportar bloqueio, neutralização e remoção de malware, notificação de administradores.

17.18. A solução deve permitir que os administradores vejam a estrutura de administração física e lógica conforme ela é apresentada no VMware vCenter.

17.19. A solução deve fornecer ao administrador informações detalhadas sobre eventos em máquinas virtuais e a implementação de tarefas.

17.20. A solução deve permitir que os administradores apliquem diferentes configurações de segurança para diferentes grupos de máquinas virtuais.

17.21. A solução deve permitir que os administradores excluam da proteção arquivos com um nome específico, arquivos localizados em um endereço específico e arquivos com uma máscara específica.

17.22. A solução deve permitir que os administradores exportem/importem uma lista de exceções.

17.23. A solução deve incluir a lista de exceções frequentes compiladas de acordo com as recomendações da Microsoft.

17.24. A solução deve permitir que os administradores verifiquem as unidades de rede conectadas à máquina virtual protegida, se necessário.

17.25. A solução deve permitir que os administradores excluam as unidades de rede da proteção.

17.26. A solução deve oferecer suporte para VMware vMotion .

17.27. A solução deve oferecer suporte para VMware DRS.

17.28. A solução deve oferecer suporte ao armazenamento de cópias de backup de arquivos excluídos.

17.29. A solução deve suportar um esquema de licenciamento de acordo com o número de máquinas virtuais protegidas e de acordo com o número de núcleos de CPU de hardware.

17.30. A solução deve ter um componente dedicado para integração centralizada com o ambiente virtual que reduza a carga no servidor VMware vCenter excluindo chamadas de outros componentes de proteção antimalware.

17.31. A solução deve oferecer suporte para ativação usando um código de ativação fornecido na assinatura.

17.32. A solução deve fornecer informações sobre o número de objetos verificados.

17.33. A solução deve fornecer informações sobre os detalhes do banco de dados de antivírus.

17.34. A solução deve oferecer suporte à verificação de certificados SSL para comunicação entre o mecanismo antimalware, o servidor de gerenciamento e os componentes da infraestrutura VMware

17.35. A solução deve permitir que os administradores importem ou exportem a lista de exclusões de verificação e proteção em tarefas de verificação e perfis de proteção

17.36. A solução deve permitir que os administradores protejam as máquinas virtuais que executam os sistemas operacionais Windows e Linux.

17.37. A solução deve permitir aos administradores a capacidade de verificar máquinas virtuais desligadas (sem colocá-las online) montando o disco da máquina virtual na máquina virtual de segurança.

17.38. A solução deve permitir que os administradores especifiquem diferentes ações para ameaças encontradas em máquinas virtuais ligadas e desligadas

17.39. A solução deve oferecer suporte ao modo multilocação - uma infraestrutura gerenciada por um VMware vCloud Director.

17.40. A solução deve ter a capacidade de verificar a reputação dos recursos da Web em relação a um banco de dados global de ameaças

17.41. A solução deve oferecer suporte à verificação de endereços da Web se eles pertencerem à categoria de endereços da Web de publicidade ou à categoria de endereços da Web associados à distribuição de aplicativos legítimos que podem ser explorados para danificar uma máquina virtual ou dados do usuário.

17.42. A solução deve ser capaz de desbloquear ataques de rede bloqueados incorretamente (Falso Positivo) sem demora

17.43. A solução deve incluir a capacidade de verificar endereços da Web em um banco de dados global de endereços de phishing

17.44. A solução deve ser capaz de restringir o acesso para configuração com base em contas de usuário

17.45. A solução deve ser capaz de verificar máquinas virtuais Linux desligadas com os seguintes sistemas de arquivos: EXT2, EXT3, EXT4, XFS, BTRFS.

17.46. A solução deve ser capaz de digitalizar modelos de máquina virtual

17.47. Quando implantada, a solução deve ser capaz de fornecer um relatório detalhado sobre quais máquinas virtuais estão protegidas/desprotegidas. E se protegido, por qual máquina virtual de segurança está protegido

17.48. A solução deve suportar o serviço SNMP. Por exemplo: Receber informações sobre o estado atual do componente IDS/IPS.

17.49. A solução deve suportar ambiente de grande escala

18. SERVIÇO DE SUPORTE

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

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

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

18.1.3. Acompanhamento nos chamados escalados para a FABRICANTE em situações de falhas/problemas desconhecidos pelo suporte técnico da LICITANTE ou bugs;

18.1.4. O atendimento deverá ser realizado via contato telefônico ou ferramenta de acesso remoto e quando necessário, on-site, independentemente do tipo de incidente;

18.1.5. Suporte técnico 8x5, prestado unicamente à equipe de segurança da área de tecnologia da contratante, referente a problemas de funcionamento/configuração dos produtos fornecidos;

18.1.6. Número de chamados ilimitados;

18.1.7. Tempo de atendimento telefônico máximo de 4 horas após a abertura do chamado técnico com a contratante;

18.1.8. Incidentes, chamados, e problemas escalados ao FABRICANTE deverão ter suporte 24x7 via web e telefone, tendo atendimento em português de segunda a sexta das 09h às 18h (horário de Brasília);

18.1.9. A Licitante deverá realizar atendimento on-site contemplando 1 (uma) visita técnica por ano, cada visita, de no mínimo 12 (doze) horas comerciais, através de um profissional certificado na solução, definidas à critério da CONTRATANTE, na sede contratante, durante a vigência das licenças (36 meses) para realizar atuações dos softwares e da console de gerenciamento e realizar o repasse de conhecimento das nova funcionalidades para equipe de TIC da contratante.

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

18.2.1. 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): 10 horas (Horário Comercial);

18.2.2. Severidade Nível 2 (Alto – Onde afeta a funcionalidade do produto mas não causa corrupção e perda de dados ou travamento sistemas): 16 horas (Horário Comercial);

18.2.3. Severidade Nível 3 (Médio – Solicitações não críticas onde não afeta a funcionalidade do produto): 24 horas (Horário Comercial);

18.2.4. 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): 32 horas (Horário Comercial).

19. RESULTADOS ESPERADOS

19.1. Maior capacidade e agilidade no atendimento às demandas do Tribunal de Contas;

19.2. Proteção do parque tecnológico contra a ação das ameaças cibernéticas.

20. MÉTODO DE SELEÇÃO E CRITÉRIO DE AVALIAÇÃO

20.1. 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, 25 de abril de 2023

Jose Alex de TI
Analista de Controle Externo - TI

ANEXO II – MODELO DE PROPOSTA

MODELO DE PROPOSTA DE PREÇO

AO TRIBUNAL DE CONTAS DO ESTADO/RN

Prezados Senhores:

Apresentamos a V. Sa nossa proposta para o objeto do **Pregão Eletrônico nº XX/2023**, declarando que temos pleno conhecimento de todos os aspectos relativos à licitação em causa e nossa plena concordância com as condições estabelecidas no Edital e seus anexos, conforme demonstrativo abaixo de nossa proposta de preço:

Empresa:
CNPJ:
Inscrição Estadual:
Endereço:
Fone: E-mail:

Representante legal:
CPF:
Fone: E-mail:

Para fins de Pagamento:
Banco:.....
Agência: .....
Conta Corrente:.....

Prazo de validade desta proposta: 60 (Sessenta) dias (mínimo).
Prazo de garantia e suporte técnico: conforme o Edital.

ITEM	DESCRIÇÃO	MARCA	QUANTIDADE / UNIDADE	PREÇO UNITÁRIO	PREÇO TOTAL

(local e data)

_____
(nome e assinatura do representante legal)

ANEXO III – ATA DE REGISTRO DE PREÇO

TRIBUNAL DE CONTAS DO ESTADO
RIO GRANDE DO NORTE

Núcleo de Contratos – NC/SG

(MINUTA DA) ATA DE REGISTRO DE PREÇOS N° 000/2023 – TC

O **TRIBUNAL DE CONTAS DO ESTADO DO RIO GRANDE DO NORTE**, inscrito no CNPJ/MF sob o nº 12.978.037/0001-78, com sede na Avenida Getúlio Vargas, 690, Petrópolis, CEP 59012-360, em Natal/RN, representado, neste ato, conforme delegação de competência verificada no inciso V, do artigo 1º, da Portaria nº 003/2023-GP/TCE, publicada no Diário Eletrônico do TCE/RN, edição do dia 03 de janeiro de 2023, pelo seu Secretário Geral, RICARDO HENRIQUE DA SILVA CÂMARA, inscrito no CPF/MF sob o nº 030.275.224-26 e portador da Cédula de Identidade nº 1.694.214, expedida pela SSP/RN, em vista do resultado do PREGÃO ELETRÔNICO Nº 0XX/2023-TC, para REGISTRO DE PREÇOS, publicado no Diário Eletrônico do TCE/RN, edição do dia XX.XX.2023, de acordo com os atos do processo nº 1600/2023-TC, RESOLVE registrar os preços do fornecedor identificado e qualificado nesta ARP, segundo a classificação alcançada por ele e nas quantidades cotadas, atendendo às condições previstas no Edital, sujeitando-se as partes às normas constantes na Lei nº 10.520/2002, na Lei Complementar nº 123/2006, na Resolução nº 007/2007 e Resolução nº 009/2008, ambas de lavra do TCE/RN e, de forma subsidiária, na Lei nº 8.666/1993, devidamente atualizada, bem como às condições dispostas a seguir:

1. DO OBJETO

1.1. A presente ata tem por objeto o registro de preços para a eventual aquisição de **licenças de softwares antivírus**, conforme condições, quantidades e exigências dispostas no Termo de Referência, que, desde já, é parte integrante desta ARP, assim como a proposta vencedora da licitação, independentemente da sua transcrição.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto e as demais condições ofertadas na proposta são as que seguem:

Fornecedor: ...	
CNPJ/MF n°: ...	**Telefone:** ...
Endereço: ...	
E-mail: ...	**Cidade/Estado:** ...
Representante Legal: ...	
RG n°: ...	**CPF/MF n°:** ...

ITEM	DESCRIÇÃO	MARCA	UNID.	QUANT.	PREÇO UNITÁRIO (R$)	PREÇO TOTAL (R$)
1	Licença do software antivírus Kaspersky endpoint security for business advanced (PLUS), pelo período de 36 meses.	Kaspersky	Unidade	700	...	...

2	Licença do software antivírus Kaspersky Hybrid Cloud Security CPU Standard (PLUS), pelo período de 36 meses	Kaspersky	Unidade	10	...	...
						VALOR TOTAL: R$ 00,00 (...)

3. DA UTILIZAÇÃO DA ATA POR TERCEIROS

3.1. Não será admitida a utilização da presente ARP por qualquer órgão ou entidade da Administração Pública, ou seja, ficam vedadas aquisições e contratações adicionais.

4. VALIDADE DA ATA

4.1. A validade da presente ARP será de 12 (doze) meses, a partir da data de sua assinatura pelas partes envolvidas, não podendo ser prorrogada.

5. SUSPENSÃO E CANCELAMENTO

5.1. Os preços registrados poderão ser suspensos quando:

5.1.1. O Tribunal de Contas julgar que o fornecedor esteja temporariamente impossibilitado de cumprir as exigências do Edital, ressalvadas as contratações já levadas a efeito até a data da decisão; e

5.1.2. Mediante solicitação por escrito do fornecedor, desde que o mesmo comprove a impossibilidade de cumprimento das exigências do Edital, motivada por causa superveniente e estranha a sua vontade, ficando sujeito às penalidades previstas no instrumento convocatório respectivo.

5.2. O fornecedor terá o seu registro cancelado quando:

5.2.1. descumprir as exigências do instrumento convocatório que deu origem ao registro de preços;

5.2.2. não assinar o Termo de Contrato decorrente do registro de preços ou não retirar, no prazo estabelecido pelo Tribunal, o instrumento equivalente, dentre os previstos no art. 62 da Lei nº 8.666/1993, salvo se aceita sua justificativa;

5.2.3. não aceitar reduzir o preço registrado, na hipótese de este se tornar superior àqueles praticados no mercado;

5.2.4. der causa a rescisão administrativa de contrato decorrente do registro de preços;

5.2.5. ocorrer qualquer das hipóteses de inexecução total ou parcial de contrato, relativamente a contratação decorrente do registro de preços por ele formalizada; ou

5.2.6. tiver presente razões de interesse público, devidamente fundamentadas, ou houver hipótese prevista em lei.

5.3. O cancelamento de registros nas hipóteses previstas nos itens 5.2.1 a 5.2.6 será formalizado por despacho da autoridade competente do Secretário Geral e a comunicação ao fornecedor interessado acerca da decisão tomada, juntando-se comprovante desta nos autos, assegurados o contraditório e a ampla defesa.

5.4. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ARP, devidamente comprovados e justificados:

5.4.1. por razão de interesse público; ou

5.4.2. a pedido do fornecedor.

5.5. Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o Setor Gerenciador convocará o(s) fornecedor(es) para negociar(em) a redução dos preços aos valores praticados pelo mercado.

5.6. O fornecedor que não aceitar reduzir seu preço ao valor praticado pelo mercado será liberado do compromisso assumido.

5.7. Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor não puder cumprir o compromisso, o Setor Gerenciador poderá:

5.7.1. liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

5.7.2. convocar os demais fornecedores, obedecida a ordem de classificação, para assegurar igual oportunidade de negociação.

5.8. Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação desta ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

5.9. As alterações de preços serão registradas em ARP complementar.

6. DO FORO

6.1. Fica eleito o foro da Justiça Estadual, Comarca de Natal, Estado do Rio Grande do Norte, para dirimir quaisquer dúvidas e litígios decorrentes desta ARP, com exclusão de qualquer outro, por mais privilegiado que seja.

7. CONDIÇÕES GERAIS

7.1. As condições gerais do fornecimento, tais como os prazos para entrega e recebimento do objeto, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Edital e seus anexos;

7.2. O Tribunal de Contas não se obriga a adquirir o item registrado do licitante vencedor, nem tampouco, as quantidades previstas, conforme art. 15, § 4º da Lei nº 8.666, de 1993, bem como o art. 20 da Resolução n.º 007/2007 – TCE/RN.

Para firmeza e validade do pactuado, a presente ARP, depois de lida e achada em ordem, segue assinada pelas partes envolvidas para a produção dos seus devidos efeitos.

Natal/RN, XX de xxxxxxxx de 2023

_____
Secretário Geral do TCE/RN

_____
Representante Legal do Fornecedor

ANEXO IV – ORDEM DE COMPRA

TRIBUNAL DE CONTAS DO ESTADO
RIO GRANDE DO NORTE

Núcleo de Contratos – NC/SG

TRIBUNAL DE CONTAS DO ESTADO
RIO GRANDE DO NORTE

Diretoria de Administração Geral – DAG
Coordenadoria de Compras e Suprimentos – CCS

ORDEM DE COMPRA

NÚMERO:	EMISSÃO:
000	00.00.2023

DA CONTRATAÇÃO					
Licitação:	Pregão Eletrônico nº 010/2021-TC			**Homologação:**	
Processo:	1600/2023-TC	**Utilização do SRP:**	Sim	**Número da Ata:**	

DO CONTRATANTE*					
Razão Social:	Tribunal de Contas do Estado do Rio Grande do Norte – TCE/RN			**CNPJ/MF:**	12.978.037/0001-78
Endereço:	Avenida Getúlio Vargas, nº 690	**Bairro:**	Petrópolis	**CEP:**	59.012-360
Cidade/UF:	Natal/RN	**Telefone:**	(84) 3642-7368	**e-mail:**	ccs@tce.rn.gov.br
* Os dados do CONTRATANTE devem ser utilizados para fins de faturamento da Nota Fiscal.					

DO(A) CONTRATADO(A)			
Razão Social:			
Endereço:		**Bairro:**	
Cidade/UF:		**CEP:**	
Telefone/Fax:		**E-mail:**	
CNPJ/MF:		**Inscrição Estadual:**	
Representante:		**CPF/MF:**	

DO OBJETO				
Item	**Descrição:**	**Unidade**	**Quantidade**	**Preço Unitário**
-	-	-	-	-
Valor Total:				

DA DOTAÇÃO ORÇAMENTÁRIA	
Órgão/Unidade:	02101 – Tribunal de Contas o Estado
Função/Sub-Função/Programa:	01.122.0100 – Programa de Gestão, Manutenção e Serviços ao Estado
Projeto/Atividade:	202101 – Manutenção e Funcionamento
Natureza da Despesa:	3390.40 – Serviços de Tec. da Informação e Comunicação – Pessoa Jurídica
Fonte de Recursos:	0.100 – Recursos Ordinários

DAS CONDIÇÕES GERAIS

1 – Pagamento:

1.1. O pagamento será efetuado por meio de ordem bancária a favor do(a) CONTRATADO(A), em prazo condizente com o estabelecido na Resolução nº 021/2016-TCE, de 06 de setembro de 2016, que será contado da data de liquidação da Nota Fiscal/Fatura, que deve indicar, obrigatoriamente, BANCO, AGÊNCIA, CONTA e TITULAR para recebimento do crédito, e ser protocolada, após o

devido recebimento do objeto, em campo próprio no sítio eletrônico do CONTRATANTE (http://www.tce.rn.gov.br/NotaFiscal/Index), em conformidade com as instruções ali fixadas;

1.2. O documento fiscal não aprovado pelo órgão competente do CONTRATANTE será devolvido ao(à) CONTRATADO(A) para as necessárias correções, com as informações que motivaram sua rejeição, contando-se os prazos estabelecidos para pagamento a partir da data de sua reapresentação;

1.3. O CONTRATANTE prorrogará o pagamento para o primeiro dia útil subsequente, caso a data estabelecida para a sua realização coincida com dias feriados ou sem expediente bancário;

1.4. No valor total do objeto já estão incluídos os impostos federais, estaduais e municipais, bem como possíveis despesas com embalagens, transporte e seguros e, ainda, os custos referentes a quaisquer outros encargos sociais, trabalhistas, previdenciários, tributários, fiscais e comerciais.

2 – Entrega e recebimento:

2.1. O objeto do presente instrumento deverá ser entregue no endereço do CONTRATANTE conforme prazo estipulado no Termo de Referência da contratação ou, na ausência de tal previsão, em até 30 (trinta) dias corridos da data do recebimento, segundo as orientações do servidor designado para o seu acompanhamento e fiscalização, e de acordo com as especificações do processo licitatório;

2.2. Será rejeitado, no todo ou em parte, conforme o caso, o objeto entregue em desacordo com a contratação, cabendo ao(à) CONTRATADO(A) todos os ônus decorrentes de tal rejeição**;**

2.3. O(A) CONTRATADO(A) deverá substituir o produto que esteja em desconformidade com o estabelecido no processo licitatório, notadamente nas especificações do Termo de Referência, no prazo máximo de 5 (cinco) dias úteis, contados da notificação feita pelo CONTRATANTE;

3 – Obrigações das partes:

3.1. São obrigações do CONTRATANTE: (a) efetuar os pagamentos devidos na forma ajustada; (b) assegurar, no que couber, as condições necessárias para a regular cumprimento do objeto contratado e; (c) designar um representante para fiscalizar e acompanhar a execução do objeto;

3.2. São obrigações do(a) CONTRATADO(A): (a) cumprir o objeto deste instrumento de acordo com as condições pactuadas; (b) manter, durante toda a execução deste instrumento, em compatibilidade com as obrigações por ele(a) assumidas, todas as condições de habilitação e qualificação exigidas para a contratação; (c) apresentar, sempre que solicitado, documentos que comprovem estar cumprindo a legislação em vigor quanto aos encargos sociais, trabalhistas, previdenciários, tributários, fiscais e comerciais, assumidos como de sua inteira responsabilidade, durante a execução deste instrumento; (d) assumir inteira responsabilidade civil, administrativa e penal por qualquer dano e/ou prejuízo causado por atos praticados por seus empregados ou prepostos durante a execução do objeto deste instrumento.

4 – Penalidades:

4.1. O descumprimento total ou parcial das obrigações assumidas pelo(a) CONTRATADO(A) poderá ensejar a aplicação das penalidades previstas nos artigos 86 a 88 da Lei nº 8.666/1993, inclusive multa;

4.2. As multas serão de 0,5% ao dia pelo atraso na execução do objeto deste instrumento, calculadas sobre o seu valor total atualizado ou da parte não cumprida, até o limite de 2% (dois por cento), salvo motivo justificado, comprovado e acolhido pelo CONTRATANTE e, não obstante, se der causa à rescisão antecipada do presente instrumento, o(a) CONTRATADO(A) incorrerá em multa de 2% (dois por cento) sobre o valor total atualizado deste instrumento;

4.3. As penalidades decorrentes de fatos diversos serão consideradas independentes entre si e poderão ser cumuladas com as de multa, que poderão ser descontadas dos pagamentos a serem efetuados.

5 – Rescisão

5.1. O presente instrumento poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666/1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo das penalidades cabíveis;

5.2. Ficam reconhecidos os direitos do CONTRATANTE no caso de rescisão administrativa prevista no

art. 77 da Lei nº 8.666/1993 e, de igual modo, o direito do(a) CONTRATADO(A) à previa e ampla defesa, razão pela qual os casos de rescisão serão formalmente motivados e comunicados por escrito.

6 – Foro

6.1. O Foro para solução de litígios decorrentes do presente instrumento será o da Justiça Estadual, Comarca de Natal, Rio Grande do Norte, com a exclusão de qualquer outro, por mais privilegiado que seja.

7 – Disposições complementares

7.1. O presente instrumento vincula-se ao edital da licitação e seus anexos ou, se for o caso, ao termo de dispensa ou inexigibilidade e seus anexos, identificados no campo DA CONTRATAÇÃO, bem como à proposta vencedora, independentemente de transcrição e sem prejuízo de suas disposições;

7.2. Aplicam-se na execução do presente instrumento, inclusive em relação aos casos omissos, as disposições da Lei nº 8.666/1993, das Resoluções do TCE/RN e demais normas aplicáveis à matéria e, subsidiariamente, as disposições da Lei nº 8.078/1990 e normas e princípios gerais dos contratos;

7.3. O presente instrumento constitui modelo simplificado de contrato e foi celebrado de acordo com a parte final do art. 62 da Lei nº 8.666/1993, devendo o respectivo número e o da correspondente Nota de Empenho constar, obrigatoriamente, de todos os documentos expedidos pelo(a) CONTRATADO(A).

Emissor da Ordem de Compra*:	Matrícula:	Cargo/Função:
Fernando Antônio Teixeira Leão	9956-2	Coordenador de Compras e Suprimentos

***** assinado eletronicamente

DESPACHO DO RESPONSÁVEL PELA AUTORIZAÇÃO DE COMPRA*:

Autorizo a efetivação da aquisição do(s) objeto(s) discriminado(s) no presente instrumento, de acordo com os termos e fundamentos nele dispostos, em conformidade com o respectivo processo licitatório, assim como nas normas da legislação aplicável à execução da despesa pública orçamentária.

Natal/RN, XX de XXXXXXX de 2023

Ricardo Henrique da Silva Câmara
Secretário Geral do TCE/RN

***** assinado eletronicamente