PREGÃO
ELETRÔNICO
COADM 90006/2024

CONTRATANTE (UASG)

(UASG 990141- COORDENADORIA DE ADMINSTRAÇÃO)
(UGE 130102 - COORDENADORIA DE ADMINSTRAÇÃO)

OBJETO

Constituição de Sistema de Registro de Preços, para eventual e futura contratação de licenças de software de segurança, incluindo serviços de instalação, configuração e suporte, treinamento e atualização do software.

VALOR TOTAL DA CONTRATAÇÃO
R$ 374.853.788,73

DATA DA SESSÃO PÚBLICA
Dia ***20/09/2024*** *às* ***10h*** **(horário de Brasília)**

CRITÉRIO DE JULGAMENTO:
Menor preço

MODO DE DISPUTA:
Aberto

PREFERÊNCIA ME/EPP/EQUIPARADAS
NÃO

Baixe o app Compras.gov.br
e apresente sua proposta

Aprovado pela Secretaria de Gestão e Inovação

Sumário

1. DO OBJETO....3
2. DO REGISTRO DE PREÇOS 3
3. DA PARTICIPAÇÃO NA LICITAÇÃO....3
4. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO...5
5. DO PREENCHIMENTO DA PROPOSTA....8
6. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES 10
7. DA FASE DE JULGAMENTO....15
8. DA FASE DE HABILITAÇÃO 22
9. DA ATA DE REGISTRO DE PREÇOS....24
10. DA FORMAÇÃO DO CADASTRO DE RESERVA 25
11. DOS RECURSOS 26
12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES....27
13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO....30
14. DAS DISPOSIÇÕES GERAIS....31

GOVERNO DO ESTADO DE SÃO PAULO

SECRETARIA DE AGRICULTURA E ABASTECIMENTO

PREGÃO ELETRÔNICO COADM Nº *90006/2024*

(Processo Administrativo nº 007.00023837/2024-15)

Torna-se público que a SECRETARIA DE AGRICULTURA E ABASTECIMENTO, por meio daa COORDENADORIA DE ADMINISTRAÇÃO, sediada na Praça Ramos de Azevedo, nº 254, Centro, CEP: 01037-912 – São Paulo – SP, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Decreto estadual nº 67.608, de 27 de março de 2023, da Instrução Normativa SEGES/ME nº 73, de 30 de setembro de 2022, e demais normas da legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital e em seus Anexos.

1. DO OBJETO

O objeto da presente licitação é a Constituição de Sistema de Registro de Preços, para eventual e futura contratação de licenças de software de segurança, incluindo serviços de instalação, configuração e suporte, treinamento e atualização do software.

1.1. Conforme condições, quantidades e exigências estabelecidas neste Edital e seus Anexos.

1.2. A licitação será realizada em grupo único, formados por 11 itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

2. DO REGISTRO DE PREÇOS

2.1. Tratando-se de licitação para registro de preços, as regras referentes aos órgãos ou entidades gerenciadoras e participante (s), bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços apresentada como Anexo deste Edital.

3. DA PARTICIPAÇÃO NA LICITAÇÃO

3.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

3.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

3.1.2. 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.

3.2. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no subitem anterior 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.

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

3.4. Nos limites previstos no art. 4º da Lei nº 14.133, de 2021, e na Lei Complementar nº 123, de 14 de dezembro de 2006, serão observadas, caso aplicáveis, as regras de tratamento favorecido para as microempresas e empresas de pequeno porte, para as cooperativas que atendam ao disposto no art. 34 da Lei n° 11.488, de 15 de junho de 2007, e no art. 16 da Lei nº 14.133, de 2021, para o agricultor familiar, para o produtor rural pessoa física e para o microempreendedor individual – MEI.

3.5. Em relação às regras aplicáveis à presente licitação concernentes a tratamento favorecido para as microempresas, empresas de pequeno porte e equiparadas, observa-se que:

3.5.1. *Para o grupo único, a participação é ampla, sendo aplicáveis as regras de tratamento favorecido constantes dos arts. 42 a 45 da Lei Complementar nº 123, de 2006, observado o disposto no § 2º do art. 4º da Lei nº 14.133, de 2021.*

3.5.2. *Considerando o valor estimado do* grupo único o *objeto desta licitação, não se aplicam a ele as regras de tratamento favorecido constantes dos arts. 42 a 49 da Lei Complementar nº 123, de 2006, nos termos dos §§ 1º e 3º do art. 4º da Lei nº 14.133, de 2021.*

3.6. Não poderão disputar esta licitação:

3.6.1. aquele que não atenda às condições deste Edital e seu(s) Anexo(s);

3.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados, observado o disposto nos §§ 2º e 4º do art. 14 da Lei nº 14.133, de 2021;

3.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários, observado o disposto nos §§ 2º e 4º do art. 14 da Lei nº 14.133, de 2021;

3.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

3.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

3.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

3.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

3.6.8. agente público do órgão ou entidade licitante;

3.6.9. aquele que não tenha representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente.

3.7. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade licitante ou contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

3.7.1. A vedação de participação de agente público do órgão ou entidade licitante ou contratante de que trata o subitem anterior estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3.8. O impedimento decorrente de imposição de sanção de que trata o subitem 3.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.9. No que concerne aos subitens 3.6.2 e 3.6.3, equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

3.10. *Será permitida a participação de sociedades cooperativas nesta licitação, nos termos do art. 16 da Lei nº 14.133, de 2021.*

3.11. *Será admitida a participação de pessoas jurídicas em consórcio, nos termos do art. 15 da Lei nº 14.133, de 2021.*

3.11.1. *Será vedada a participação de empresa consorciada, na mesma licitação, de mais de um consórcio ou de forma isolada, nos termos do art. 15, inc. IV, da Lei nº 14.133, de 2021.*

4. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

4.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

4.1.1. As disposições deste Edital que tratam especificamente da forma de realização da fase de habilitação são aplicáveis na hipótese em que a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento (caso assim definido no subitem 4.1), se ausente previsão expressa em sentido diverso. Como exceção a essas disposições, na hipótese em que seja adotado procedimento com fase de habilitação antecedente (caso assim definido no subitem 4.1), segue-se disciplina específica neste Edital conforme disposições que contêm previsão expressa de aplicação a essa última hipótese.

4.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto (conforme a alternativa adequada ao critério de julgamento definido no início deste Edital, correspondendo ao menor preço ou maior desconto, respectivamente), até a data e o horário estabelecidos para abertura da sessão pública.

4.2.1. Caso seja definido no subitem 4.1 que a fase de habilitação antecederá a fase de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no subitem anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto (conforme o critério de julgamento definido no início deste Edital), admitindo-se que a documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira seja substituída pelo registro cadastral no Sicaf, e observado o disposto no inc. III do art. 63 da Lei nº 14.133, de 2021.

4.3. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

4.3.1. está ciente e concorda com as condições contidas no Edital e seus Anexos, bem como que a proposta apresentada compreenderá a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

4.3.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição Federal;

4.3.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

4.3.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

4.4. O licitante organizado em cooperativa (se admitida a participação de cooperativa no item 3) deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

4.5. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa que atenda ao disposto no art. 34 da Lei nº 11.488, de 2007 (se admitida a participação de cooperativa no item 3) deverá declarar, ainda, em campo próprio

do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º da Lei n.º 14.133, de 2021, excetuada a hipótese de se verificar uma das exceções dos §§ 1º ao 3º do art. 4º supracitado, conforme especificado nos subitens 4.5.1 e 4.5.2 subsequentes.

4.5.1. Não se aplica o tratamento favorecido estabelecido nos arts. 42 a 49 da Lei Complementar nº 123, de 2006, na hipótese em que item objeto desta licitação tenha valor estimado superior ao limite estabelecido nos §§ 1º e 3º do art. 4º da Lei nº 14.133, de 2021, conforme seja especificado, quando houver, no item 3.

4.5.2. Não têm direito ao tratamento favorecido estabelecido nos arts. 42 a 49 da Lei Complementar nº 123, de 2006, as microempresas, as empresas de pequeno porte e as cooperativas (se admitida a participação de cooperativas) que, no ano-calendário de realização da licitação, tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, nos termos do § 2º do art. 4º da Lei nº 14.133, de 2021.

4.5.3. Na hipótese de se verificar uma das exceções especificadas no subitem 4.5.1 ou no subitem 4.5.2, o licitante deverá assinalar o campo “não”, por não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006.

4.5.4. No item exclusivo para participação de microempresas, empresas de pequeno porte e equiparadas, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item.

4.5.5. Nos itens em que a participação não for exclusiva para microempresas, empresas de pequeno porte e equiparadas, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa equiparada (se admitida a participação de cooperativa).

4.6. A falsidade da declaração de que trata os subitens 4.3 a 4.5 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

4.7. Os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema, até a abertura da sessão pública.

4.7.1. Caso seja definido no subitem 4.1 que a fase de habilitação antecederá a fase de apresentação de propostas e lances, os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

4.8. Não haverá ordem de classificação na etapa de apresentação da proposta pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

4.8.1. Caso seja definido no subitem 4.1 que a fase de habilitação antecederá a fase de apresentação de propostas e lances, não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

4.9. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

4.10. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo (conforme a alternativa adequada ao critério de julgamento definido no início deste Edital, correspondendo ao menor preço ou maior desconto, respectivamente) quando do cadastramento da proposta e obedecerá às seguintes regras:

4.10.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

4.10.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

4.11. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

4.11.1. valor superior a lance já registrado pelo fornecedor no sistema, quando definido no início deste Edital o critério de julgamento por menor preço; e

4.11.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando definido no início deste Edital o critério de julgamento por maior desconto.

4.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do subitem 4.10 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

4.13. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

4.14. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

5. DO PREENCHIMENTO DA PROPOSTA

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

5.1.1. *Valor unitário e total do total*

5.1.2. *Marca;*

5.1.3. *Fabricante;*

5.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

5.2.1. *Nesta licitação para registro de preços, o* licitante não poderá oferecer proposta em quantitativo inferior ao máximo previsto para futura contratação, nos termos da documentação que constitui Anexo deste Edital.

5.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

5.4. 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.

5.5. Independentemente do percentual de tributo inserido na planilha, quando houver determinação legal de retenção de tributo, no pagamento serão retidos na fonte os percentuais que sejam estabelecidos na legislação vigente.

5.6. As microempresas e empresas de pequeno porte impedidas de optar pelo Simples Nacional, ante as vedações previstas na Lei Complementar nº 123, de 2006, não poderão aplicar os benefícios decorrentes desse regime tributário diferenciado em sua proposta, devendo elaborá-la de acordo com as normas aplicáveis às demais pessoas jurídicas.

5.6.1. Quando for o caso, e se vier a ser contratado, o licitante na situação descrita no subitem anterior deverá requerer ao órgão fazendário competente a sua exclusão do Simples Nacional até o último dia útil do mês subsequente àquele em que ocorrida a situação de vedação, nos termos do art. 30, *caput*, inc. II, e § 1º, inc. II, da Lei Complementar nº 123, de 2006, apresentando à Administração a comprovação da exclusão ou o seu respectivo protocolo.

5.6.2. Se o Contratado não realizar espontaneamente o requerimento de que trata o subitem anterior, caberá ao ente público contratante comunicar o fato ao órgão fazendário competente, solicitando que o Contratado seja excluído de ofício do Simples Nacional, nos termos do art. 29, inc. I, da Lei Complementar nº 123, de 2006.

5.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe a documentação que integra este Edital, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de utilizar os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

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

5.9. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas, quando participarem de licitações públicas.

5.9.1. Caso seja definido no início deste Edital o critério de julgamento por maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos no subitem anterior.

5.10. O descumprimento das regras supramencionadas por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas competente e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição Federal, e do art. 33, inc. X, da Constituição do Estado de São Paulo; ou condenação dos agentes públicos responsáveis e do contratado ao pagamento de indenização pelos

prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

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

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

6.2. Os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema, até a abertura da sessão pública.

6.2.1. Caso seja definido no subitem 4.1 que a fase de habilitação antecede a fase de apresentação de propostas e lances, os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

6.3. O sistema disponibilizará campo próprio para troca de mensagens entre o pregoeiro e os licitantes.

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

6.5. O lance deverá ser ofertado pelo valor unitário do item.

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

6.7. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema (conforme a alternativa adequada ao critério de julgamento definido no início deste Edital, correspondendo ao menor peço ou maior desconto, respectivamente).

6.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de:

Item 1: R$ 5,00 (cinco reais);

Item 2: R$ 55,00 (cinquenta e cinco reais);

Item 3: R$ 10,00 (dez reais);

Item 4: R$ 1,00 (um real);

Item 5: R$ 10,00 (dez reais);

Item 6: R$ 240,00 (duzentos e quarenta reais);

Item 7: R$ 10.000,00 (dez mil reais);

Item 8: R$ 5,00 (cinco reais);

Item 9: R$ 10,00 (dez reais);

Item 10: R$ 2,00 (dois reais);

Item 11: R$ 160,00 (cento e sessenta reais).

6.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

6.10. O procedimento seguirá de acordo com o modo de disputa adotado, definido no início deste Edital.

6.11. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

6.11.1. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

6.11.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

6.11.3. Não havendo novos lances na forma estabelecida nos subitens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

6.11.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

6.11.5. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

6.12. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

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

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

6.12.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

6.12.4. Não havendo pelo menos três ofertas nas condições definidas nos dois subitens anteriores, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

6.12.5. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

6.13. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “fechado e aberto”, poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço/ maior percentual de desconto e os das propostas até 10% (dez por cento) superiores/inferiores àquela (conforme a alternativa adequada ao critério de julgamento definido no início deste Edital), em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

6.13.1. Não havendo pelo menos 3 (três) propostas nas condições definidas no subitem anterior, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

6.13.2. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

6.13.3. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

6.13.4. Não havendo novos lances na forma estabelecida nos subitens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

6.13.5. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

6.13.6. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

6.14. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

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

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

6.17. No caso de desconexão com o pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

6.18. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

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

6.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006.

6.20.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

6.20.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

6.20.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

6.20.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

6.20.5. Não se aplica o tratamento favorecido estabelecido nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, na hipótese em que item objeto desta licitação tenha

valor estimado superior ao limite estabelecido nos §§ 1º e 3º do art. 4º da Lei nº 14.133, de 2021, conforme seja especificado, quando houver, no item 3.

6.21. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

6.21.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

6.21.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

6.21.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos na Lei nº 14.133, de 2021;

6.21.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

6.21.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

6.21.2. Persistindo o empate, será assegurada preferência, nos termos do § 1º do art. 60 da Lei nº 14.133, de 2021, sucessivamente, aos bens e serviços produzidos ou prestados por:

6.21.2.1. empresas estabelecidas no território do Estado de São Paulo;

6.21.2.2. empresas brasileiras;

6.21.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

6.21.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

6.22. Encerrada a etapa de envio de lances da sessão pública, na hipótese de a proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto mínimo definido para a contratação (conforme a alternativa adequada ao critério de julgamento estabelecido no início deste Edital), o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

6.22.1. *Neste certame para registro de preços, tratando-se de licitação por grupo de itens:*

6.22.1.1. serão observados como critério de aceitabilidade de preços unitários máximos:

R$ 498,00 (quatrocentos e noventa e oito reais);

R$ 10.450 (dez mil e quatrocentos e cinquenta reais);

R$ 1.298,00 (mil e duzentos e noventa e oito reais);

R$ 119,67 (cento e dezenove reais e sessenta e sete centavos);

R$ 1.474,00 (mil e quatrocentos e setenta e quatro reais);

R$ 46.585,67 (quarenta e seis mil e quinhentos e oitenta e cinco reais e sessenta e sete centavos);

R$ 2.981.292,33 (dois milhões e novecentos e oitenta e um mil e duzentos e noventa e dois reais e trinta e três centavos);

R$ 200,33 (duzentos reais e trinta e três centavos);

R$ 1.954,33 (mil e novecentos e cinquenta e quatro reais e trinta e três centavos);

R$ 304,00 (trezentos e quatro reais);

R$ 31.194,67 (trinta e um mil e cento e noventa e quatro reais e sessenta e sete centavos);

6.22.1.1. a contratação posterior de item específico do grupo exigirá prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou entidade.

6.22.2. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

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

6.22.4. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

6.22.5. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de *2 (duas) horas*, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

6.22.6. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante antes de findo o prazo, ou de ofício, a critério do pregoeiro, quando constatado que o prazo estabelecido não é suficiente para o envio da documentação exigida.

6.23. Após a negociação do preço, o pregoeiro iniciará a fase de aceitação e julgamento da proposta.

7. DA FASE DE JULGAMENTO

7.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133, de 2021, legislação correlata e no subitem 3.6 deste Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1. SICAF;

7.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/sancoes/consulta);

7.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/sancoes/consulta);

7.1.4. Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade – CNCIAI, do Conselho Nacional de Justiça (http://www.cnj.jus.br/improbidade_adm/consultar_requerido.php);

7.1.5. Sistema Eletrônico de Aplicação e Registro de Sanções Administrativas – e-Sanções (http://www.esancoes.sp.gov.br);

7.1.6. Cadastro Estadual de Empresas Punidas – CEEP (http://www.servicos.controladoriageral.sp.gov.br/PesquisaCEEP.aspx); e

7.1.7. Relação de apenados publicada pelo Tribunal de Contas do Estado de São Paulo (https://www.tce.sp.gov.br/apenados).

7.2. A consulta ao cadastro CNCIAI será realizada em nome da pessoa jurídica licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992.

7.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 29, *caput*, c/c Decreto estadual nº 67.608, de 2023)

7.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 29, § 1º, c/c Decreto estadual nº 67.608, de 2023).

7.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 29, § 2º, c/c Decreto estadual nº 67.608, de 2023).

7.3.3. Constatada a existência de sanção, o licitante será considerado inabilitado, por falta de condição de participação.

7.4. Caso atendidas as condições de participação, prosseguirá a análise da fase de julgamento da proposta classificada em primeiro lugar.

7.4.1. O disposto nos subitens 7.4 e 7.6.2 será excepcionado se for definido no subitem 4.1 que a fase de habilitação antecede a fase de apresentação de propostas e lances, hipótese em que, caso atendidas as condições de participação, será iniciado o procedimento de habilitação, nos termos do item 8, antes de se realizar a fase de julgamento.

Qualificação Técnica

7.4.2. Comprovação de capacidade operacional para execução de fornecimento similar de complexidade tecnológica e operacional equivalente ou superior ao objeto desta contratação, ou ao item pertinente, por meio da apresentação de certidão(ões) ou atestado(s), fornecido(s) por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

7.4.2.1. Para fins da comprovação de que trata este subitem, o(s) atestado(s) ou certidão(ões) deverá(ão) dizer respeito a contrato(s) executado(s) com a(s) seguinte(s) característica(s) mínima(s):

7.4.2.1.1. A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de solução de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets ou similar à proposta, em ambiente compatível ao da CONTRATANTE, contendo no mínimo 40.000 (quarenta mil) ativos monitorados.

7.4.2.1.2. A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de solução de segurança e antivírus para servidores em cloud ou similar à proposta, em ambiente compatível ao da CONTRATANTE, contendo no mínimo 2.000 (dois mil) ativos monitorados.

7.4.2.1.3. A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de solução de segurança antispam/mail gateway para e-mail ou similar à proposta, em ambiente compatível ao da CONTRATANTE, contendo no mínimo 15.000 (quinze mil) caixas postais monitoradas.

7.4.2.1.4. A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de serviço de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets, em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano), em ambiente compatível ao da CONTRATANTE, contendo no mínimo 20.000 (vinte mil) ativos monitorados;

7.4.2.1.5. A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de solução de monitoramento com, no mínimo, 250 (duzentos e cinquenta) ativos de rede, servidores e aplicações monitorados.

7.4.2.1.6. A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de solução de Service Desk para abertura e resolução de chamados de no mínimo, 750 (setecentos e cinquenta) usuários.

7.4.2.1.7. Será admitida, para fins de comprovação de quantitativo mínimo de fornecimento similar, a apresentação e o somatório de diferentes certidões ou atestados de fornecimentos executados de forma concomitante.

7.4.2.1.8. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

7.4.2.1.9. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade do(s) atestado(s), apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

7.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido a microempresas e empresas de pequeno porte, o pregoeiro verificará se faz jus ao benefício, em conformidade com os subitens 3.5 e 4.5 deste Edital.

7.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro 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.

7.6.1. Se a proposta vencedora for desclassificada, o pregoeiro examinará a proposta subsequente, e, assim sucessivamente, na ordem de classificação.

7.6.2. Encerrada a fase de julgamento, caso se verifique a conformidade da proposta de que trata o subitem 7.6, o pregoeiro passará à verificação da documentação de habilitação do licitante conforme disposições do item 8.

7.7. Será desclassificada a proposta vencedora que:

7.7.1. contiver vícios insanáveis;

7.7.2. não obedecer às especificações técnicas pormenorizadas neste Edital ou em seus Anexos;

7.7.3. apresentar preços inexequíveis ou permanecer acima do preço máximo definido para a contratação;

7.7.4. não tiver sua exequibilidade demonstrada, quando exigido pela Administração;

7.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus Anexos, desde que insanável.

7.8. Caso seja definido no item 1 que o objeto da licitação consiste em fornecimento de bens ou prestação de serviços em geral (não definidos como serviços de engenharia), serão considerados indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

7.8.1. A inexequibilidade, na hipótese de que trata o subitem anterior, só será considerada após diligência do pregoeiro, que comprove:

7.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e

7.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

7.9. Caso seja definido no item 1 que o objeto da licitação consiste em prestação de serviços de engenharia, além das disposições acima, a análise de exequibilidade e sobrepreço considerará o seguinte:

7.9.1. Caso seja definido pela documentação que integra este Edital que o regime de execução será contratação por tarefa, empreitada por preço global ou empreitada integral, a caracterização do sobrepreço se dará pela superação do valor global estimado.

7.9.2. Caso seja definido pela documentação que integra este Edital que o regime de execução será empreitada por preço unitário, a caracterização do sobrepreço se dará pela superação do valor global estimado *e pela superação de custo unitário tido como relevante, conforme documentação e planilha anexadas a este Edital.*

7.9.3. Serão consideradas inexequíveis as propostas cujos valores forem inferiores a 75% (setenta e cinco por cento) do valor orçado pela Administração, observado o disposto no subitem subsequente.

7.9.3.1. A inexequibilidade, na hipótese de proposta cujo valor seja inferior a 75% (setenta e cinco por cento) do valor orçado pela Administração, só será considerada após diligência do pregoeiro, facultando ao licitante comprovar, no prazo assinalado pela Administração, a viabilidade dos preços constantes em sua proposta, sob pena de desclassificação.

7.9.4. Será exigida garantia adicional do licitante vencedor cuja proposta for inferior a 85% (oitenta e cinco por cento) do valor orçado pela Administração, equivalente à diferença entre este último e o valor da proposta, sem prejuízo das demais garantias exigíveis de acordo com a Lei.

7.10. Caso seja definido no item 1 que o objeto da licitação consiste em prestação de serviços contínuos com regime de dedicação exclusiva ou predominância de mão de obra (sejam serviços em geral ou de engenharia), além das disposições acima, deverão ser observados os seguintes preceitos:

7.10.1. A análise da exequibilidade da proposta de preços deverá ser realizada com o auxílio de planilha de custos e formação de preços, a ser preenchida pelo licitante em relação à sua proposta final, conforme modelo constante de Anexo deste Edital.

7.10.2. A apresentação de valores abaixo dos respectivos custos referentes a itens isolados da planilha de custos e formação de preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

7.10.3. É vedado ao licitante incluir na planilha de custos e formação de preços:

a) item relativo a despesas decorrentes de disposições contidas em acordos, convenções ou dissídios coletivos de trabalho que tratem de matéria não trabalhista, de pagamento de participação dos trabalhadores nos lucros ou resultados do contratado, ou que estabeleçam direitos não previstos em lei, tais como valores ou índices obrigatórios de encargos sociais ou previdenciários, bem como de preços para os insumos relacionados ao exercício da atividade (art. 135, § 1º, da Lei nº 14.133, de 2021);

b) item relativo a despesas decorrentes de disposições contidas em acordos, convenções ou dissídios coletivos de trabalho que tratem de obrigações e direitos que somente se aplicam aos contratos com a Administração Pública (art. 135, § 2º, da Lei nº 14.133, de 2021).

7.10.4. A inclusão na proposta de item de custo vedado não acarretará a desclassificação do licitante, devendo o pregoeiro determinar que o respectivo custo seja excluído da planilha, observando-se o disposto no inciso III do art. 12 da Lei nº 14.133, de 2021.

7.10.5. Na hipótese de contratação com a previsão de itens de custos vedados, tais valores serão glosados e os itens serão excluídos da planilha, garantidos ampla defesa e contraditório.

7.10.6. O licitante vencedor deverá indicar os sindicatos, acordo(s) coletivo(s), convenção(ões) coletiva(s) ou sentença(s) normativa(s) que regem a(s) categoria(s) profissional(is) que executará(ão) o serviço e a(s) respectiva(s) data(s)-base(s) e vigência(s), com base na Classificação Brasileira de Ocupações – CBO.

7.10.7. Em todo caso, deverá ser garantido o pagamento do salário normativo previsto no instrumento coletivo aplicável ou do salário-mínimo vigente, o que for maior.

7.10.8. Caso seja definido no item 1 que o objeto da licitação consiste em prestação de serviços contínuos com regime de dedicação exclusiva de mão de obra (sejam serviços em geral ou de engenharia), cuja produtividade seja mensurável e indicada na documentação que integra este Edital, o licitante deverá indicar a produtividade adotada e a quantidade de pessoal que será alocado na execução contratual.

7.10.8.1. Caso a produtividade seja diferente daquela utilizada pela Administração como referência, ou não esteja contida na faixa referencial de produtividade, mas seja admitida pelo Edital, o licitante deverá apresentar a respectiva comprovação de exequibilidade.

7.10.8.2. Os licitantes poderão apresentar produtividades diferenciadas daquela estabelecida pela Administração como referência, desde que não alterem o objeto da contratação, não contrariem dispositivos legais vigentes e, caso não estejam contidas nas faixas referenciais de produtividade, comprovem a exequibilidade da proposta.

7.10.8.3. Para efeito do subitem anterior, admite-se a adequação técnica da metodologia empregada pelo licitante, visando assegurar a execução do objeto, desde que mantidas as condições para a justa remuneração do serviço.

7.11. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que o licitante comprove a exequibilidade da proposta.

7.12. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços ou outra espécie de planilha elaborada pela Administração conforme documentação anexada a este Edital, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

7.12.1. Caso seja definido no item 1 que o objeto da licitação consiste em prestação de serviços de engenharia, o licitante vencedor será convocado a apresentar à Administração, por meio eletrônico, as planilhas com indicação dos quantitativos e dos custos unitários, seguindo o modelo elaborado pela Administração conforme documentação anexada a este Edital, bem como com detalhamento das Bonificações e Despesas Indiretas (BDI) e dos Encargos Sociais (ES), com os respectivos valores adequados ao valor final da proposta vencedora, nos termos do disposto no § 5º do art. 56 da Lei nº 14.133, de 2021.

7.13. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação.

7.13.1. O ajuste de que trata o subitem anterior se limita a sanar erros ou falhas que não alterem a substância das propostas.

7.13.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

7.14. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

7.15. Caso seja estabelecida a exigência de apresentação de amostra(s) ou de execução de prova de conceito na documentação que integra este Edital como Anexo considerando o objeto da licitação, por ocasião do julgamento das propostas, será exigido do licitante classificado em primeiro lugar a sua realização, conforme procedimento disciplinado na documentação que integra este Edital como Anexo, sob pena de não aceitação da proposta.

7.15.1. Por meio de mensagem no sistema, será divulgado o local, data e horário de realização do procedimento para a avaliação da(s) amostra(s) ou para a execução da prova de conceito (em conformidade com a exigência estabelecida no Edital), cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

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

7.15.3. Caso se trate de exigência de apresentação de amostra(s), se não houver entrega da(s) amostra(s) ou se ocorrer atraso na entrega, sem justificativa aceita pelo pregoeiro, ou se houver entrega de amostra(s) fora das especificações previstas neste Edital, a proposta do licitante será recusada.

7.15.3.1. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o pregoeiro 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 na documentação que integra este Edital como Anexo.

7.15.4. Caso se trate de exigência de execução de prova de conceito, não será aceita a proposta do licitante que tiver a prova de conceito rejeitada, que não a realizar ou que não a realizar nas condições estabelecidas na documentação que integra este Edital como Anexo.

7.15.4.1. No caso de desclassificação do licitante, o pregoeiro convocará o próximo licitante, obedecida a ordem de classificação, sucessivamente, até que um licitante cumpra os requisitos e funcionalidades previstas na prova de conceito.

7.16. Requisitos de Experiência Profissional Os serviços de suporte e garantia referente a solução de segurança, deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços; Comprovação de o licitante possui, em seu quadro de funcionários, na data prevista para a entrega da proposta, profissional de nível superior ou outro devidamente reconhecido pela respectiva entidade profissional competente e que seja certificado pelo fabricante dos produtos objeto desta licitação, e/ou a comprovação da disponibidade do

profissional mediante contrato de prestação de serviços, sem vinculo trabalhista e regido pela legislação Civil. Deverá apresentar a certificação do(s) técnico(s) mediante certificados emitidos pelo fabricante.

8. DA FASE DE HABILITAÇÃO

8.1. Os documentos que serão exigidos para fins de habilitação estão especificados na documentação que constitui Anexo deste Edital, consistindo na documentação necessária e suficiente para demonstrar a capacidade do licitante de realizar o objeto da licitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

8.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

8.1.2. Nesta licitação, não haverá exigência de que o licitante ateste, sob pena de inabilitação, que conhece o local e as condições de realização do objeto, ou que tem conhecimento pleno das condições e peculiaridades da contratação.

8.1.3. Se for permitida a participação de pessoas jurídicas em consórcio no item 3, para efeito de habilitação técnica, caso exigida na documentação que integra este Edital como Anexo, será admitido o somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, caso exigida na documentação que integra este Edital como Anexo, será admitido o somatório dos valores de cada consorciado.

8.1.3.1. Na hipótese de admissão da participação de pessoas jurídicas em consórcio e exigência de requisito de habilitação econômico-financeira de que trata o subitem anterior, se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte, haverá um acréscimo de 10% para o consórcio em relação ao valor exigido dos licitantes individuais para habilitação econômico-financeira.

8.2. Os documentos exigidos para fins de habilitação poderão ser apresentados em original ou por cópia.

8.3. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133, de 2021.

8.4. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133, de 2021).

8.5. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

8.6. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

8.7. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

8.7.1. 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 ou quando a lei expressamente o exigir. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 4º, § 1º, e art. 6º, § 4º, c/c Decreto estadual nº 67.608, de 2023).

8.8. É de responsabilidade do licitante 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. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 7º, *caput*, c/c Decreto estadual nº 67.608, de 2023).

8.8.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 7º, parágrafo único, c/c Decreto estadual nº 67.608, de 2023).

8.9. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

8.9.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de *2 (duas) horas*, prorrogável por igual período, contado da solicitação do pregoeiro.

8.9.2. O disposto nos subitens 8.9.1 e 8.13 será excepcionado se for definido no subitem 4.1 que a fase de habilitação antecederá a fase de apresentação de propostas e lances, hipótese em que os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto (conforme a alternativa adequada ao critério de julgamento definido no início deste Edital), observado o disposto nos subitens 8.1.1 e 8.3.

8.10. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

8.10.1. Os documentos relativos à regularidade fiscal especificados na documentação que integra este Edital como Anexo somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

8.10.2. O disposto no subitem 8.10 será excepcionado se for definido no subitem 4.1 que a fase de habilitação antecederá a fase de apresentação de propostas e lances, hipótese em que a verificação no Sicaf ou a exigência dos documentos nele não contidos ocorrerá em relação a todos os licitantes, respeitada a exceção do subitem 8.10.1.

8.11. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei nº 14.133, de 2021, art. 64):

8.11.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

8.11.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

8.12. Na análise dos documentos de habilitação, o pregoeiro poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

8.13. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente Edital, observado o prazo definido no subitem 8.9.1.

8.14. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao Edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

8.15. A comprovação de regularidade fiscal e trabalhista das microempresas, das empresas de pequeno porte e das cooperativas que atendam ao disposto no art. 34 da Lei n° 11.488, de 2007 (se admitida a participação de cooperativas no item 3) somente será exigida para efeito de contratação, e não como condição para participação na licitação, exceto na hipótese em que item objeto desta licitação tenha valor estimado superior ao limite estabelecido nos §§ 1º e 3º do art. 4º da Lei nº 14.133, de 2021, conforme seja especificado, quando houver, no item 3.

8.15.1. Havendo alguma restrição no que tange à regularidade fiscal e trabalhista, o licitante habilitado nas condições do subitem anterior deverá comprovar sua regularização sob pena de decadência, sem prejuízo da aplicação das sanções cabíveis, mediante a apresentação das competentes certidões negativas de débitos, ou positivas com efeito de negativa, no prazo de 5 (cinco) dias úteis, contado a partir do momento em que o licitante for declarado vencedor do certame, prorrogável por igual período, a critério da Administração.

8.16. Caso seja definido no subitem 4.1 que a fase de habilitação antecederá a fase de apresentação de propostas e lances, quando a fase de habilitação já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

8.17. A disciplina da adjudicação, da homologação e da contratação (esta última não aplicável a licitações para registro de preços) encontra-se no item 14 deste Edital.

9. DA ATA DE REGISTRO DE PREÇOS

9.1. *Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 05 (cinco) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, conforme minuta que integra este Edital como Anexo, sob pena de decadência do direito, sem prejuízo das sanções previstas na* Lei nº 14.133, de 2021.

9.1.1. *O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:*

a) a solicitação seja devidamente justificada e apresentada dentro do prazo; e

b) a justificativa apresentada seja aceita pela Administração.

9.1.2. *A ata de registro de preços será assinada com a utilização de meio eletrônico, nos termos da legislação aplicável, e disponibilizada no sistema de registro de preços.*

9.2. *Serão formalizadas tantas Atas de Registro de Preços quantas forem necessárias para o registro de todos os itens constantes na documentação que integra este Edital, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.*

9.3. *O preço registrado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência da ata de registro de preços.*

9.4. *A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a contratação pretendida, desde que devidamente justificada.*

9.5. *Na hipótese de o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidas neste item 9, a Administração poderá convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado, observado o disposto no item 10 deste Edital.*

10. DA FORMAÇÃO DO CADASTRO DE RESERVA

10.1. *Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro:*

a) dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e

b) dos licitantes que mantiverem sua proposta original.

10.2. *As contratações respeitarão a ordem de classificação dos licitantes registrados na ata.*

10.2.1. *A apresentação de novas propostas dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário na forma da alínea "a" do subitem anterior não prejudicará o resultado do certame em relação ao licitante mais bem classificado.*

10.2.2. *Os licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário antecederão, na ordem de classificação, aqueles que mantiverem sua proposta original.*

10.3. *A fase de apresentação de amostra(s) ou de execução de prova de conceito que seja exigida na documentação que integra este Edital, quando houver, e a habilitação dos licitantes que comporão o cadastro de reserva serão efetuadas quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:*

a) quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidos neste Edital; ou

b) quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas no item 9 da Ata de Registro de Preços, conforme minuta que integra este Edital como Anexo.

10.4. *Na hipótese de nenhum dos licitantes que aceitaram cotar o objeto com preço igual ao do adjudicatário concordar com a contratação em igual prazo e nas condições propostas pelo primeiro classificado, a Administração, observados o valor estimado e a sua eventual atualização na forma prevista na documentação que integra este Edital, poderá:*

a) convocar os licitantes que mantiveram sua proposta original para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário;

b) adjudicar e celebrar a contratação nas condições ofertadas pelos licitantes remanescentes, observados o disposto neste item 10 e a ordem de classificação, quando frustrada a negociação de melhor condição.

11. DOS RECURSOS

11.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

11.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

11.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

11.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

11.3.2. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos;

11.3.3. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

11.3.4. em exceção ao disposto no subitem 11.3.3, se for definido no subitem 4.1 que a fase de habilitação antecede a fase de apresentação de propostas e lances, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

11.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

11.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar o recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

11.6. Os recursos interpostos fora do prazo não serão conhecidos.

11.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da

interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.8. O recurso terá efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

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

11.10. Os autos do processo permanecerão com vista franqueada aos interessados *pelo meio eletrônico* **crprecos@sp.gov.br**

12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

12.1. Comete infração administrativa, nos termos da lei, o licitante ou contratado que, com dolo ou culpa:

12.1.1. der causa à inexecução parcial do contrato;

12.1.2. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

12.1.3. der causa à inexecução total do contrato;

12.1.4. deixar de entregar a documentação exigida para o certame, inclusive não entregar qualquer documento que tenha sido solicitado pelo pregoeiro durante o certame;

12.1.5. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta, em especial quando:

12.1.5.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

12.1.5.2. recusar-se a enviar o detalhamento da proposta quando exigível;

12.1.5.3. pedir para ser desclassificado quando encerrada a etapa competitiva;

12.1.5.4. deixar de apresentar amostra, caso exigida na documentação que integra este Edital; ou

12.1.5.5. caso exigida na documentação que integra este Edital, apresentar amostra em desacordo com as especificações do Edital;

12.1.6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

12.1.6.1. recusar-se, sem justificativa, a formalizar a contratação ou a ata de registro de preço (caso o item 1 defina licitação para registro de preços) no prazo e condições estabelecidos pela Administração;

12.1.7. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

12.1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

12.1.9. fraudar a licitação ou praticar ato fraudulento na execução do contrato;

12.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

12.1.10.1. agir em conluio ou em desconformidade com a lei;

12.1.10.2. induzir deliberadamente a erro no julgamento;

12.1.10.3. caso exigida na documentação que integra este Edital, apresentar amostra falsificada ou deteriorada;

12.1.11. praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

12.1.12. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

12.2. Com fundamento na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes, adjudicatários e/ou contratado as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

12.2.1. advertência;

12.2.2. multa;

12.2.3. impedimento de licitar e contratar; e

12.2.4. declaração de inidoneidade para licitar ou contratar.

12.3. Na aplicação das sanções serão considerados:

12.3.1. a natureza e a gravidade da infração cometida;

12.3.2. as peculiaridades do caso concreto;

12.3.3. as circunstâncias agravantes ou atenuantes;

12.3.4. os danos que dela provierem para a Administração Pública;

12.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.4. *A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial.*

12.4.1. Para as infrações previstas nos itens 12.1.1, 12.1.2 e 12.1.3, a multa será de 10% (dez por cento) do valor do contrato licitado.

12.4.2. Para as infrações previstas nos itens 12.1.4, 12.1.5, 12.1.6, 12.1.7 e 12.1.8, a multa será de 20% (vinte por cento) do valor do contrato licitado.

12.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas cumulativamente com a penalidade de multa, garantido o exercício de prévia e ampla defesa.

12.6. Antes da aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

12.7. A sanção de advertência será aplicada, após regular processo administrativo, ao responsável em decorrência da infração administrativa relacionada no subitem 12.1.1, quando não se justificar a imposição de penalidade mais grave.

12.8. A sanção de impedimento de licitar e contratar será aplicada, após regular processo administrativo, ao responsável em decorrência das infrações administrativas relacionadas nos subitens12.1.2, 12.1.3, 12.1.4, 12.1.5, 12.1.6 e 12.1.7, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do Estado de São Paulo, pelo prazo máximo de 3 (três) anos.

12.9. A sanção de declaração de inidoneidade para licitar ou contratar será aplicada, após regular processo administrativo, ao responsável em decorrência das infrações administrativas relacionadas nos subitens 12.1.8, 12.1.9, 12.1.10, 12.1.11 e 12.1.12, bem como das infrações administrativas previstas nos subitens12.1.2, 12.1.3, 12.1.4, 12.1.5, 12.1.6 e 12.1.7 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja extensão e duração observará o prazo previsto no art. 156, § 5º, da Lei n.º 14.133, de 2021.

12.10. A recusa injustificada do adjudicatário em formalizar a contratação ou assinar a ata de registro de preços (caso o item 1 defina licitação para registro de preços) no prazo e condições estabelecidos pela Administração, descrita no subitem 12.1.6.1, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas (art. 90, § 5º, da Lei nº 14.133, de 2021).

12.11. A apuração de responsabilidade relacionada às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta nos termos do art. 158 da Lei nº 14.133, de 2021, que avaliará fatos e circunstâncias conhecidos e intimará o licitante, o adjudicatário ou o contratado para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

12.12. As sanções são autônomas e a aplicação de uma não exclui a de outra.

12.13. Da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, caberá recurso no prazo de 15 (quinze) dias úteis, contado da data da intimação, observando-se o disposto no art. 166 da Lei nº 14.133, de 2021.

12.14. Da aplicação da sanção de declaração de inidoneidade para licitar ou contratar, caberá pedido de reconsideração no prazo de 15 (quinze) dias úteis, contado da data da intimação, observando-se o disposto no art. 167 da Lei nº 14.133, de 2021.

12.15. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

12.16. A aplicação das sanções previstas neste Edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados à Administração Pública.

12.17. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante à Contratada, além da perda desse valor, a diferença será descontada da garantia prestada, caso exigida na documentação que integra o Edital, ou, quando for o caso, será cobrada judicialmente (art. 156, § 8º, da Lei nº 14.133, de 2021).

12.18. Os atos previstos como infrações administrativas na lei de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846,

de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei.

12.19. A personalidade jurídica poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos na Lei nº 14.133, de 2021, ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia, nos termos do art. 160 do referido diploma legal.

12.20. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo federal (art. 161 da Lei nº 14.133, de 2021).

12.21. *Caso o item 1 defina licitação para registro de preços:*

12.21.1. *Será da competência do órgão ou entidade gerenciadora, garantidos o contraditório e a ampla defesa, aplicar as penalidades decorrentes de infrações no procedimento licitatório, do descumprimento do pactuado na ata de registro de preço, em relação à sua demanda registrada, ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações.*

12.21.2. *Será da competência do respectivo órgão ou entidade participante, garantidos o contraditório e a ampla defesa, aplicar as penalidades decorrentes do descumprimento do pactuado na ata de registro de preço, em relação à sua demanda registrada, ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações.*

12.21.3. *O órgão ou entidade participante deverá informar ao órgão ou entidade gerenciadora as ocorrências descritas no subitem anterior.*

13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

13.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, ou para solicitar esclarecimento sobre os seus termos, devendo protocolar a impugnação ou o pedido de esclarecimento até 3 (três) dias úteis antes da data da abertura do certame.

13.2. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, *pelo seguinte meio*: **crprecos@sp.gov.br**

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

13.3.1. A concessão de efeito suspensivo à impugnação é medida excepcional, e, caso ocorra, será motivada nos autos do processo de licitação.

13.4. A decisão da impugnação ou a resposta ao pedido de esclarecimento serão divulgadas em sítio eletrônico oficial conforme especificado no subitem subsequente, no

prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

13.4.1. As decisões das impugnações e as respostas aos pedidos de esclarecimento serão juntadas aos autos do processo licitatório, ficarão disponíveis para consulta por qualquer interessado, e serão publicadas *no sistema e no endereço eletrônico na Internet* **crprecos@sp.gov.br**, sem informar a identidade do responsável pela impugnação ou pelo pedido de esclarecimento.

13.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame, exceto quando a alteração não comprometer a formulação das propostas.

13.6. A ausência de impugnação implicará na aceitação tácita, pelo licitante, das condições previstas neste Edital e em seus Anexos.

13.7. A ausência de pedido de esclarecimento implicará na presunção de que os interessados não tiveram dúvidas a respeito da presente licitação, razão pela qual não serão admitidos questionamentos extemporâneos.

14. DAS DISPOSIÇÕES GERAIS

14.1. Exaurida a fase recursal, será observado o disposto no art. 71 da Lei nº 14.133, de 2021.

14.1.1. Constatada a regularidade dos atos praticados, a autoridade superior adjudicará o objeto da licitação ao licitante vencedor e homologará o procedimento licitatório.

14.2. *Caso o item 1 não defina licitação para registro de preços, a disciplina da formalização da contratação observará o disposto nas subdivisões deste item 14.2.*

14.2.1. *Após a homologação da licitação, em sendo realizada a contratação, sua formalização ocorrerá mediante a assinatura de Termo de Contrato, cuja minuta integra este Edital como Anexo.*

14.2.1.1. Se, por ocasião da formalização da contratação, algum dos documentos apresentados pelo adjudicatário para fins de comprovação das condições de habilitação estiver com o prazo de validade expirado, a Administração verificará a situação por meio eletrônico hábil de informações e certificará a regularidade nos autos do processo, anexando a ele os documentos comprobatórios, salvo impossibilidade devidamente justificada.

14.2.1.2. Se não for possível atualizar os documentos referidos no subitem anterior por meio eletrônico hábil de informações, o adjudicatário será notificado para, no prazo de 02 (dois) dias úteis, comprovar a sua situação de regularidade mediante a apresentação das certidões respectivas com prazos de validade em plena vigência, sob pena de a contratação não se realizar.

14.2.1.3. Constitui condição para a celebração da contratação, bem como para a realização dos pagamentos dela decorrentes, a inexistência de registros em nome do adjudicatário no "Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais – CADIN ESTADUAL". Esta condição será considerada

cumprida se o devedor comprovar que os respectivos registros se encontram suspensos, nos termos do art. 8º, §§ 1º e 2º, da Lei estadual nº 12.799, de 2008.

14.2.1.4. Com a finalidade de verificar se o licitante mantém as condições de participação no certame, serão novamente consultados, previamente à celebração da contratação, os cadastros especificados no item 7.1 deste Edital.

14.2.1.5. Constitui(em), igualmente, condição(ões) para a celebração da contratação:

14.2.1.5.1. a apresentação do(s) documento(s) que o adjudicatário, à época do certame licitatório, houver se comprometido a exibir por ocasião da celebração da contratação por meio de declaração específica, caso exigida na documentação que integra este Edital como Anexo;

14.2.1.5.2. a indicação de gestor encarregado de representar o adjudicatário com exclusividade perante o contratante, caso se trate de sociedade cooperativa (se admitida a participação de cooperativa);

14.2.1.5.3. caso seja definido no item 1 deste Edital que o objeto da licitação consiste em prestação de serviços de engenharia, a apresentação do registro ou inscrição do licitante no Conselho Regional de Engenharia e Agronomia – CREA ou no Conselho de Arquitetura e Urbanismo – CAU competente, com o visto do CREA/SP ou do CAU/SP, conforme o caso, se o local do registro ou inscrição for situado em região não compreendida na área de jurisdição da referida entidade, observada a legislação aplicável.

14.2.2. *O adjudicatário terá o prazo de 05 (cinco) dias, contados a partir da data de sua convocação, para assinar o Termo de Contrato, sob pena de decadência do direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.*

14.2.2.1. O contrato será assinado com a utilização de meio eletrônico, nos termos da legislação aplicável.

14.2.2.2. O prazo para assinatura previsto no subitem anterior poderá ser prorrogado por igual período, por solicitação justificada do interessado e aceita pela Administração.

14.2.2.3. Será considerado celebrado o contrato, em caso de assinaturas por meio eletrônico em datas diferentes, na data da última assinatura eletrônica das partes do termo contratual.

14.2.3. *Na hipótese de o vencedor da licitação não comprovar manter as condições de habilitação e preencher as condições de contratação consignadas neste Edital, ou não assinar o contrato, ou recusar a contratação, a Administração, sem prejuízo da apuração do cabimento de aplicação de sanções e das demais cominações legais cabíveis a esse licitante, poderá convocar os licitantes remanescentes, respeitada a ordem de classificação, para a celebração do contrato em conformidade com o procedimento e as condições estabelecidas no art. 90 da Lei nº 14.133, de 2021.*

14.2.4. *Será facultada à Administração a convocação dos demais licitantes classificados para a contratação de remanescente em consequência de rescisão de*

contrato celebrado com fundamento nesta licitação, observados os critérios estabelecidos no § 7º do art. 90 da Lei nº 14.133, de 2021.

14.3. Será divulgada ata da sessão pública no sistema eletrônico.

14.4. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo pregoeiro.

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

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

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

14.8. Os casos omissos serão solucionados pelo pregoeiro.

14.9. 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.

14.10. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

14.11. No julgamento das propostas e da habilitação, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

14.11.1. As falhas passíveis de saneamento na documentação apresentada pelo licitante são aquelas cujo conteúdo retrate situação fática ou jurídica já existente na data da abertura da sessão pública deste Pregão.

14.11.2. 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, nos termos do inciso III do art. 12 da Lei nº 14.133, de 2021.

14.12. Caso seja vencedor da licitação, o licitante a ser contratado estará sujeito à assinatura de Termo de Ciência e de Notificação, quando prevista a sua apresentação em ato normativo editado pelo Tribunal de Contas do Estado de São Paulo, conforme a disciplina aplicável.

14.13. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) *e no endereço eletrônico* **crprecos@sp.gov.br**

14.14. Para dirimir quaisquer questões decorrentes da licitação, não resolvidas na esfera administrativa, será competente o foro da Comarca da Capital do Estado de São Paulo.

14.15. Integram este Edital, para todos os fins e efeitos, os seguintes Anexos:

14.15.1. *ANEXO I - Termo de Referência;*

14.15.2. *Anexo I.1. Estudo Técnico Preliminar (ETP);*

14.15.3. *Anexo I.2. Relação de órgãos participantes;*

14.15.4. *ANEXO II – Minuta de Termo de Contrato;*

14.15.5. *ANEXO III – Modelos(s) referente(s) a planilha de proposta;*

14.15.6. *ANEXO I V – Modelo(s) de Declaração(ões);*

14.15.7. *ANEXO V – Minuta de Ata de Registro de Preços.*

São Paulo, *04 de setembro* de 20*24*

RICARDO LORENZINI BASTOS

ANEXO I

TERMO DE REFERÊNCIA COMPRAS DE TIC – LEI 14.133/2021
SECRETARIA DE AGRICULTURA E ABASTECIMENTO

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
18/2024	130222-ESP-COORD. DE TECNOL. DA INFORMACAO	ELIENE SUZANA VEIGA DE LIMA	08/08/2024 16:21 (v 10.1)

Status
PUBLICADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC		007.00023837/2024-15

1. Definição do objeto

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Constituição de Sistema de Registro de Preços para contratação eventual e futura de licenças de software de segurança, incluindo serviços de instalação, configuração e suporte, treinamento e atualização do software, nos termos da tabela abaixo, conforme condições e exigênciasestabelecidas neste instrumento.

	DESCRIÇÃO	U.F	CATMAT	QTD TOTAL	VALOR UNITÁRIO	VALOR TOTAL
1	Software de segurança e antivírus para servidores físicos, microcomputadores e smartphones /tablets com detecção e resposta e software de AntiSpam/proteçãopara o Microsoft office 365	Unidade	27464	120891	R$ 498,00	R$ 60.203.718,00
2	Software de segurança e antivíruspara ambientes virtualizados on premise	Unidade	27464	2249	R$ 10.450,00	R$ 23.502.050,00
3	Software de segurança e antivíruspara ambientes virtualizados em cloud	Unidade	27464	1649	R$ 1.298,00	R$ 2.140.402,00
4	Software de complemento de detecção e resposta para os itens02 e 03	Unidade	27464	5621	R$ 119,67	R$ 672.665,07
5	Software de detecção e respostagerenciado	Unidade	27464	54067	R$ 1.474,00	R$ 79.694.758,00
6	Software de segurança paraStorage	Unidade	27464	769	R$ 46.585,67	R$ 35.824.380,23
7	Software de detecção contra- ataques complexos e direcionados	Unidade	27464	22	R$ 2.981.292,33	R$ 65.588.431,26
8	Software de prevenção contra a perda de dados	Unidade	27464	58178	R$ 200,33	R$ 11.654.798,74
9	Software de monitoramento de aplicações e infraestrutura de redes e servidores	Unidade	27464	40262	R$ 1.954,33	R$ 78.685.234,46
10	Serviços de Instalação e Configuração	Unid. Serviço Técnico	26972	5167	R$ 304,00	R$ 1.570.768,00

11	Treinamentos dos Softwares Licenciados	Unidade	3840	491	R$ 31.194,67	R$ 15.316.582,97
	TOTAL					**R$ 374.853.788,73**

* O detalhamento dos itens, por entidade, está no Anexo I

1.1.1. Em caso de eventual divergência entre a descrição do item do catálogo do sistema Compras. gov.br e as disposições deste Termo de Referência, prevalecem as disposições deste Termo de Referência.

1.1.2. Este Termo de Referência foi elaborado em conformidade com o Decreto estadual nº 68.185, de 11 de dezembro de 2023.

1.1.3. Os bens objeto desta contratação são caracterizados como comum, conforme justificativa constante do Estudo Técnico Preliminar, elaborado nos termos do Decreto estadual nº 68.017, de11 de outubro de 2023.

1.2. O prazo de vigência da contratação é de 36 (trinta e seis) meses contados da assinatura do contrato, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

1.3. O fornecimento de bens é enquadrado como continuado tendo em vista que pode ser objetivamente especificado por meio de padrões usuais no mercado e o Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivoprocesso de contratação.

1.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigênciada contratação.

1.5. Detalhamento por órgão / entidade

	1	2	3	4	5	6	7	8	9	10	11
DESCRIÇÃO	Software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets com detecção e resposta e software de AntiSpam/proteção para o Microsoft office 365	Software de segurança e antivírus para ambientes virtualizados on premise	Software de segurança e antivírus para ambientes virtualizados em cloud	Software de complemento de detecção e resposta para os itens 02 e 03	Software de detecção e resposta gerenciado	Software de segurança para Storage	Software de detecção contra-ataques complexos e direcionados	Software de prevenção contra a perda de dados	Software de monitoramento de aplicações e infraestrutura de redes e servidores	Serviços de Instalação e Configuração	Treinamentos dos Softwares Licenciados
U.F	Unidade	Unidade	Unidade	Unidade	Unidade	Unidade	Unidade	Unidade	Unidade	Unid. Serviço Técnico	Unidade
90102 - ESP-COORD. GERAL ADMINIST. - CGA	2000	30	20	200	2000	4	1	2000	2000	100	4
90107 - ESP-CTO. VIGILANCIA SANITARIA	300	10	10	20	1	1	1	300	300	140	10
90110 - ESP-CTO. REFERENCIA E TREINAMENTO-DST/AIDS	500	64			1	1	1	1	1	80	2
90112 - ESP-GABINETE DO COORDENADOR SEC. SAUDE 1	10	10	10	10	10	10	1	10	10	10	10
90115 - ESP-DEPTO.REG.SAUDE - DRS-VI BAURU	1									1	1
90117 - ESP-DEPTO.REG.SAUDE - DRS XI PRES.PRUDENTE	100	1		1						8	1
90118 - ESP-HOSP.GERAL PREF. MIGUEL GUALDA DE PROMIS	150									10	
90120 - ESP-HOSP.EST. DR.OSWALDO B. FARIA - MIRANDOPOL	120							120	120	2	
90121 - ESP-HOSP. REGIONAL DE ASSIS	370								1	50	
90122 - ESP-HOSP. DR.ODILO A.SIQUEIRA, P.PRUDENTE	82							5	1	13	1
90124 - ESP-DEPTO.REG.SAUDE - DRS-V BARRETOS	90										
90125 - ESP-DEPTO.REG.SAUDE - DRS-VIII FRANCA	75				1		1	1	1	3	1
90126 - ESP-DEPTO.REG.SAUDE DRS-XIII RIB.PRETO	100								1	8	1
90127 - ESP-DEPTO.REG.SAUDE - DRS-XV SJRPRETO	170									25	1
90129 - ESP-HOSP. STA.TEREZA, RIB.PRETO	250	6	6	1	1	1	1	250	250	24	3
90130 - ESP-CTO.ATENCAO INTEGRAL A SAUDE S.RITA	110	3		7		1		1	1	16	2
90131 - ESP-DEPTO.REG.S	60	5	5	1	1	5	1	10	10	30	20

AUDE - DRS-VII CAMPINAS	60	5	5	1	1	5	1	10	10	30	20
90132 - ESP-DEPTO.REG.SAUDE - DRS-X PIRACICABA	220								2	33	2
90135 - ESP-DEPTO.REG.SAUDE DE TAUBATE - DRS-XVII	135									2	
90138 - ESP-DEPTO.REG.SAUDE - DRS-IV BAIXADA SANTISTA	140							140			2
90139 - ESP-DEPTO.REG.SAUDE - DRS-XVI SOROCABA	106									106	1
90141 - ESP-HOSP. GUILHERME ALVARO, SANTOS	250	3						50	3	4	1
90145 - ESP-CAIS - PROF. CANTIDIO DE MOURA CAMPOS	120								1		
90146 - ESP-CTO. REABILITACAO DE CASA BRANCA	300										1
90154 - ESP-HOSP. GERAL DE VILA NOVA CACHOEIRINHA	300	10		10	300	1			50	10	1
90155 - ESP-HOSPITAL GERAL DE TAIPAS	310	2			300			300	1	50	1
90157 - ESP-HOSP. REGIONAL SUL	280	280	280	280	280	280	1	280	280	280	280
90158 - ESP-HOSP.GERAL J.TEIXEIRA DA COSTA,EM GUAIAN	220					1			1	16	2
90159 - ESP-HOSP. GERAL S.MATEUS, DR.MANOEL BIFULCO	350	8		8	350						1
90160 - ESP-UN. GESTAO ASSIST I-HOSP. HELIOPOLIS	100								2	2	2
90161 - ESP-UN. GESTAO ASSISTENCIAL II-HOSP. IPIRANGA	60									10	1
90162 - ESP-UN. GESTAO ASSIST.III - HOSP.INF.DA RCT YA	270	10	4	3	1	2	1	2	2	1	1
90167 - ESP-HOSP. REG. DR.VIVALDO M.SIMOES, OSASCO	395	28	28	30	395	395	1	395	573	36	1
90175-ESP-CTO.ESPECIALIZ. REABILIT DR. APC- M. CRUZE					400	3		10000	900		1
90170 - ESP-CTO.AT.INTEG.SAUDE MENTAL-DR.DAVID C.C.FI	100			10			1	100		16	2
90172 - ESP-CONJUNTO HOSPITALAR DO MANDAQUI-CHM	520	40							1	50	1
90177 - ESP-INSTITUTO ADOLFO LUTZ	1000	20			1000	4		1000	13	200	4
90180 - ESP-INSTITUTO DE SAUDE	150									4	1
90181 - ESP-INSTITUTO DANTE PAZZANESE DE CARDIOLOGIA	1300									200	1

90182 - ESP-INST. LAURO DE SOUZA LIMA, EM BAURU	200								1		
90183 - ESP-INST. INFECTOLOGIA EMILIO RIBAS	650	22									
90187 - ESP-INST.PTA DE GERIATRIA E GERONTOLOG.-IPG	200						1		4	32	6
90191 - ESP-DEPTO.REG.GRANDE SAO PAULO - DRS-I G.S.P	608	10		10						6	2
90193 - ESP-GRUPO DE GERENCIAMENTO ADMINISTRATIVO	3660	80	100	180	3660	16	1	3660	3660	280	40
90200 - ESP-GRUPO DE RESGATE - GRAU	36										
90203 - ESP-HOSP.EST.ESPEC.REAB.DR.FRANCISCO R.ARANTE	150									150	4
91101 - ESP-FUNDAÇÃO P/REM. POP.CHOPIN TAVARES DE LIM	475	25	350	40	400	2	1	475	400	1	5
102401 - ESP-CTO. EST. EDUC. TECNOL. P. SOUZA - CEETEP	65000		220	220	12000	4	1	4000	12000	1200	8
131101 - ESP-FUND.INST. TERRAS JOSE G. DA SILVA ITESP	750	8	10	10	1	4			750		
172201 - ESP-IMSTIT DE PESOS E MEDIDAS DO EST. S.PAULO	1000	1000	2	40	1000	3	1	1000	50	10	2
180101 - ESP-GABINETE DO SECRETARIO E ASSES.SEC.S.PUBL	1000	20	100	1100	1100	4	2	1000	3000	2	4
180183 - ESP-DIRETORIA TEC. INFORMACAO E COMUNICACAO	25000	60		2000	25000	2	1	25000	5000		10
201201 - ESP-FUND.SISTEMA ESTADUAL ANAL.DADOS-SEADE	300	5	30	125	10	1		270	10	400	2
252101 - ESP-AG.METROPOLITANA DA BAIXADA SANTISTA	23							23		23	1
252201 - ESP-AG. METROPOLITANA DE CAMPINAS	25							25		5	1
262101 - ESP-DEP. DE AGUAS E ENERGIA ELETRICA-DAE	1000	6		50	1050	2			1000	250	4
373401 - ESP-EMP. METROP.TRANSPORTES URBS DE SP. SA	750	200							110		
390105 - ESP-CENTRO ADMINISTRATIVO - PARCERIA INVEST.	300	15	4	315	4	2	1	10	2	20	4
392601 - ESP-AG.REG.SERV. PUBL.DELEG. TRANSP.EST.	650	38	150	150		2		50	50	40	2

SP.											
930515 - ESP-FUNDAÇAO ONCOCENTRO DE SAO PAULO	100										
990141 - ESP-COORDENADORIA DE ADMINISTRACAO	3200	180	320	500	1	8	1	3200	5000	400	20
990202 - ESP-FUNDAÇÃO C.A.S.A. - SEDE ADMINISTRAÇÃO	4500	50		300	4800	10	1	4500	4500	800	10
90179- ESP-INSTITUTO PASTEUR	200								200	8	2
QUANTIDADE TOTAL	120891	2249	1649	5621	54067	769	22	58178	40262	5167	491
VALOR UNITÁRIO	498,00	10.450,00	1.298,00	119,67	1.474,00	46.585,67	2.381.292,33	200,33	1.954,33	304,00	31.194,67
VALOR TOTAL	60.203.718,00	23.502.050,00	2.140.402,00	672.665,07	79.634.758,00	35.824.380,23	65.588.431,26	11.654.738,74	78.685.234,46	1.570.768,00	15.316.582,37

2. Fundamentação da contratação

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1.A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em Tópicoespecífico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

2.2. O objeto da contratação não está previsto no Plano de Contratações Anual 2024, considerandoque o documento foi facultativo no exercício de 2023.

2. Descrição da solução

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico doEstudo Técnico Preliminar, apêndice deste Termo de Referência.

ITEM 01 - SOFTWARE DE SEGURANÇA E ANTIVÍRUS PARA SERVIDORES FÍSICOS, MICROCOMPUTADORES E SMARTPHONES/TABLETS COM DETECÇÃO E RESPOSTA E SOFTWARE DE ANTISPAM/PROTEÇÃO PARA O MICROSOFT OFFICE 365

3.1.1. Do módulo de proteção de endpoint

3.1.1.1. A solução proposta deverá proteger os sistemas operacionais para estações de trabalho:

3.1.1.1.1. Windows 7;
3.1.1.1.2. Windows 8;

3.1.1.1.3. Windows 8.1;
3.1.1.1.4. Windows 10;
3.1.1.1.5. Windows 11;
3.1.1.2. A solução proposta deverá proteger os sistemas operacionais para servidores:
3.1.1.2.1. Windows 7 Windows Small Business Server 2011;
3.1.1.2.2. Windows MultiPoint Server 2011;

3.1.1.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022;

3.1.1.3. A solução proposta deverá proteger os servidores de terminal Microsoft:
3.1.1.3.1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008R2, 2012 R2, 2016, 2019 e 2022;
3.1.1.4. A solução proposta deverá proteger os sistemas operacionais Linux:
3.1.1.4.1. Linux Mint 20.3 e posteriores (64bits);
3.1.1.4.2. Amazon Linux 2 (64bits);
3.1.1.4.3. CentOS 6.7 e posteriores (32/64bits);
3.1.1.4.4. Debian 11 e posteriores (32/64bits);
3.1.1.4.5. OpenSUSE Leap 15 (64bits);
3.1.1.4.6. Oracle Linux 7.3 e posteriores (64bits);
3.1.1.4.7. Red Hat Enterprise Linux 6.7 e posteriores (32/64bits);
3.1.1.4.8. SUSE Server 12.5 e posteriores (64bits);
3.1.1.4.9. Ubuntu 20.04 e posteriores (64bits);

3.1.1.4.10. Rocky Linux 8.5 e posteriores

(64bits); 3.1.1.4.11. CentOS Stream 8 e

posteriores (64bits);

3.1.1.4.12. Sistemas operacionais Arm de 64 bits: CentOS Stream 9, SUSE Linux Enterprise Server15 e Ubuntu 22.04 LTS;

3.1.1.5. A solução proposta deverá proteger os sistemas operacionais MAC OS:

3.1.1.5.1. macOS 12 – 14;

3.1.1.6. Ferramentas de virtualização MAC OS:
3.1.1.6.1. Parallels Desktop 16 para Mac Business Edition;
3.1.1.6.2. VMware Fusion 11.5 Profissional;
3.1.1.6.3. VMware Fusion 12 Profissional;
3.1.1.7. A solução proposta deverá suportar as seguintes plataformas virtuais:
3.1.1.7.1. VMware Workstation 17.0.2 Pro;
3.1.1.7.2. VMware ESXi 8.0 Update 2;
3.1.1.7.3. Microsoft Hyper-V Server 2019;
3.1.1.7.4. Citrix Virtual Apps e Desktop 7 2308;
3.1.1.7.5. Citrix Provisioning 2308;
3.1.1.7.6. Citrix Hypervisor 8.2 Update 1;

3.1.2. Do módulo de gerenciamento avançado

3.1.2.1. A solução proposta deve suportar arquitetura cloud-native e On-premise;

3.1.2.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

3.1.2.2.1. Amazon Web Services;

3.1.2.2.2. Microsoft Azure;

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

3.1.2.3.1. HP (Microfoco) ArcSight;

3.1.2.3.2. IBM Qradar;

3.1.2.3.3. Splunk;

3.1.2.3.4. Kaspersky KUMA;

3.1.2.4. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes;

3.1.2.5. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança prédefinidas;

3.1.2.6. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos;

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

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

3.1.2.9. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador;

3.1.2.10. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento;

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

3.1.2.12. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis;

3.1.2.13. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem;

3.1.2.14. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

3.1.2.14.1. Status do dispositivo;

3.1.2.14.2. Tag;
3.1.2.14.3. Diretório ativo;
3.1.2.14.4. Proprietários de

dispositivos;3.1.2.14.5. Hardware;

3.1.2.15. A solução proposta deve suportar os seguintes canais de entrega de

notificação:3.1.2.15.1. E-mail;

3.1.2.15.2. Registro de

sistema;3.1.2.15.3. SMS;

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

rede;3.1.2.16.2. Nome;

3.1.2.16.3. Domínio e/ou Sufixo de Domínio;

3.1.2.16.4. Endereço de IP;

3.1.2.16.5. Endereço IP para servidor de

gerenciamento;3.1.2.16.6. Localização no Active

Directory;

3.1.2.16.7. Unidade organizacional;
3.1.2.16.8. Grupo;
3.1.2.16.9. Sistema operacional;

3.1.2.16.10. Número do pacote de

serviço;3.1.2.16.11. Arquitetura Virtual;

3.1.2.16.12. Registro de aplicativos;

3.1.2.16.13. Nome da Aplicação;

3.1.2.16.14. Versão do aplicativo;

3.1.2.16.15. Fabricante;

3.1.2.16.16. Tipo e

versão;3.1.2.16.17.

Arquitetura;

3.1.2.17. A solução proposta deve ter a capacidade de criar/definir configurações com base nalocalização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão;
3.1.2.18. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexãounidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública;
3.1.2.19. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

3.1.2.19.1. Dispositivos Desktop/Servidores;
3.1.2.19.2. Dispositivos

móveis; 3.1.2.19.3.

Dispositivos de rede;

3.1.2.19.4. Dispositivos

virtuais;

3.1.2.19.5. Componentes OEM;

3.1.2.19.6. Periféricos de computador;

3.1.2.19.7. Dispositivos IoT

conectados;3.1.2.19.8. Telefones

VoIP;

3.1.2.19.9. Repositórios de rede;

3.1.2.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:
3.1.2.20.1. Nome da Aplicação;

3.1.2.20.2. Caminho do aplicativo;

3.1.2.20.3. Metadados do aplicativo;

3.1.2.20.4. Aplicativo Certificado

digital;

3.1.2.20.5. Categorias de aplicativos predefinidas pelo

fornecedor;3.1.2.20.6. SHA256 e MD5;

3.1.2.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes

dispositivos:3.1.2.21.1. Bluetooth;

3.1.2.21.2. Dispositivos móveis;
3.1.2.21.3. Modems externos;
3.1.2.21.4. CD/DVD;
3.1.2.21.5. Câmeras e

scanners;3.1.2.21.6. MTPs;

3.1.2.21.7. E a transferência de dados para dispositivos móveis;

3.1.2.22. A solução proposta deve ter capacidade de ler informações do Active Directory para obterdados sobre contas de computadores na organização;
3.1.2.23. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão;
3.1.2.24. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:
3.1.2.24.1. Estruturas de domínios e grupos de trabalho do Windows;

3.1.2.24.2. Estruturas de grupos do Active Directory;
3.1.2.24.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador;
3.1.2.25. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização;
3.1.2.26. A solução proposta deve permitir realizar as seguintes ações para

endpoints:3.1.2.26.1. Verificação manual;

3.1.2.26.2. Verificação no acesso;

3.1.2.26.3. Verificação por demanda;

3.1.2.26.4. Verificação de arquivos compactados;

3.1.2.26.5. Verificação de arquivos individuais, pastas e

unidades;3.1.2.26.6. Bloqueio e verificação de scripts;

3.1.2.26.7. Proteção contra alteração de

registros;3.1.2.26.8. Proteção contra estouro de

buffer; 3.1.2.26.9. Verificação em segundo

plano/inativa;

3.1.2.26.10. Verificação de unidade removível na conexão com o sistema;

3.1.2.27. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou AntiMalware;
3.1.2.28. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma

determinada política/tarefa possam ser revisadas;
3.1.2.29. 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;

3.1.2.30. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc;
3.1.2.31. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração;
3.1.2.32. A solução proposta deve suportar Windows Failover Cluster ou compor com outra solução de alta disponibilidade;
3.1.2.33. A solução proposta deve ter um recurso de Clustering integrado;
3.1.2.34. A solução proposta deve incluir alguma forma de sistema para controlar epidemias devírus;
3.1.2.35. solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia;
3.1.2.36. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança;

3.1.2.37. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo;
3.1.2.38. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux;
3.1.2.39. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB;
3.1.2.40. A solução proposta deve ter capacidade de bloquear a execução de qualquer executáveldo dispositivo de armazenamento USB;
3.1.2.41. A solução proposta deve contar com filtragem de firewall por endereço local, interfacefísica e Time-ToLive (TTL) de pacotes;
3.1.2.42. A solução proposta deverá possuir controles para download de DLL e drivers;
3.1.2.43. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentrodo sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo específico de prevenção de intrusão;
3.1.2.44. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável;
3.1.2.45. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log);
3.1.2.46. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server;
3.1.2.47. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam 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;

3.1.2.48. A solução proposta deve permitir o teste de atualizações baixadas por meio do

software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las;
3.1.2.49. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior;
3.1.2.50. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários;
3.1.2.51. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança AntiMalware através do servidor de administração;
3.1.2.52. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários;
3.1.2.53. A solução proposta deve ter um mecanismo de notificação para informar os usuáriossobre eventos no software e nas configurações AntiMalware instalados, e para distribuir notificações sobre eventos por e-mail;
3.1.2.54. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados;
3.1.2.55. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração;
3.1.2.56. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal;
3.1.2.57. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software AntiMalware e dados sobre inventário de hardware e software, licenciamento etc.;
3.1.2.58. 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 definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis;
3.1.2.59. A solução proposta deve permitir ao administrador personalizar relatórios;
3.1.2.60. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluílas automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado;
3.1.2.61. A solução proposta deve permitir ao administrador definir um período após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor;
3.1.2.62. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento;
3.1.2.63. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento;
3.1.2.64. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico;
3.1.2.65. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos;
3.1.2.66. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
3.1.2.67. O servidor de gerenciamento primário 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 secundários;

3.1.2.68. A solução proposta deve suportar integração com solução APT;
3.1.2.69. A solução proposta deve suportar a integração com o serviço Managed Detection and response;

3.1.2.70. A solução proposta deve permitir instalar o modulo de gerenciamento On-premisenos seguintes sistemas operacionais:

3.1.2.70.1. Windows;
3.1.2.70.2. Linux;
3.1.2.71. A solução proposta deverá suportar os seguintes servidores de banco de dados:

3.1.2.71.1. Sistemas operacionais Windows:

3.1.2.71.1.1. Microsoft SQL Server;
3.1.2.71.1.2. Microsoft Banco de dados SQL do

Azure;3.1.2.71.1.3. MySQL Standard e Enterprise;

3.1.2.71.1.4. MariaDB;

3.1.2.71.1.5. PostgreSQL;

3.1.2.71.2. Sistemas operacionais Linux:
3.1.2.71.2.1. MySQL;
3.1.2.71.2.2. MariaDB;
3.1.2.71.2.3. PostgreSQL;
3.1.2.72. A solução proposta deverá suportar as seguintes plataformas virtuais:

3.1.2.72.1. Sistemas operacionais Windows:

3.1.2.72.1.1. VMware vSphere 6.7 e 7.0;

3.1.2.72.1.2. Estação de trabalho VMware 16

Pro;

3.1.2.72.1.3. Servidor Microsoft Hyper-V 2012 de 64 bits;
3.1.2.72.1.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;
3.1.2.72.1.5. Microsoft Servidor Hyper -V 2016 de 64 bits;
3.1.2.72.1.6. Servidor Microsoft Hyper-V 2019 de 64 bits;
3.1.2.72.1.7. Servidor Microsoft Hyper-V 2022 de 64 bits;
3.1.2.72.1.8. Citrix XenServer 7.1 LTSR;

3.1.2.72.1.9. Citrix XenServer 8.x;

3.1.2.72.1.10. Oracle VM VirtualBox 6.x;

3.1.2.72.2. Sistemas operacionais

Linux: 3.1.2.72.2.1. VMware vSphere 6.7,

7.0 e 8.0;

3.1.2.72.2.2. VMware Desktop 16 Pro e 17 Pro;

3.1.2.72.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits;
3.1.2.72.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;
3.1.2.72.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits;
3.1.2.72.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits;
3.1.2.72.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits;
3.1.2.72.2.8. Citrix XenServer 7.1 e 8.x;

3.1.2.72.2.9. Oracle VM VirtualBox 6.x

e7.x;

3.1.3. A solução proposta deve suportar criptografia ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;
3.1.3.1. A solução proposta deve suportar criptografia em vários níveis:
3.1.3.1.1. Criptografia completa do disco – incluindo disco do sistema;
3.1.3.1.2. Criptografia de arquivos e pastas;
3.1.3.1.3. Criptografia de mídia removível;
3.1.3.1.4. Gerenciamento de criptografia Bitlocker e MacOS Filevault2;
3.1.3.2. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível dearquivo (FLE) que permita:
3.1.3.2.1. A criptografia de arquivos em unidades de computador locais;
3.1.3.2.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões;
3.1.3.2.3. A criação de listas criptografadas de pastas em unidades de computador locais;
3.1.3.3. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
3.1.3.3.1. Especificar uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis;
3.1.3.3.2. Configurar regras de criptografia para arquivos armazenados em unidades removíveis individuais;
3.1.3.4. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
3.1.3.4.1. A criptografia de todos os arquivos armazenados em unidades removíveis;
3.1.3.4.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis;
3.1.3.5. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia;

3.1.3.6. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis;
3.1.3.7. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado;

3.1.3.8. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido;
3.1.3.9. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma

ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais;

3.1.3.10. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interro mper configurações de criptografia;
3.1.3.11. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados;
3.1.3.12. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema;
3.1.3.13. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado;
3.1.3.14. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário; 3.1.3.15. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados;
3.1.3.16. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos;
3.1.3.17. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação;
3.1.3.18. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário;
3.1.3.19. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de préinicialização;
3.1.3.20. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bitlocker;
3.1.3.21. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft Bitlocker, incluindo:

3.1.3.21.1. Uso do Trusted Platform Module e configurações de senha;
3.1.3.21.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software sea criptografia de hardware não estiver disponível;
3.1.3.21.3. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo,com teclados touchscreen em tablets);
3.1.3.22. A solução proposta deve suportar criptografia em Microsoft Surface Tablets;
3.1.4. A solução proposta deve suportar gerenciamento de sistemas próprio ou compor ferramenta do mesmo fabricante que tenha capacidade similar;
3.1.4.1. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
3.1.4.1.1. Instalação remota de software de terceiros;
3.1.4.1.2. Relatórios sobre software e hardware existentes;
3.1.4.1.3. Monitoramento para instalação de software não autorizado;
3.1.4.1.4. Remoção de software não autorizado;
3.1.4.2. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados;
3.1.4.3. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints;
3.1.4.4. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade;

3.1.4.5. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais;
3.1.4.6. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches;
3.1.4.7. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade;
3.1.4.8. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros;
3.1.4.9. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança;
3.1.4.10. A solução proposta deve permitir ao administrador aprovar atualizações;
3.1.4.11. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes;
3.1.4.12. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias;
3.1.4.13. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis;
3.1.4.14. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros;
3.1.4.15. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos;
3.1.4.16. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências);
3.1.4.17. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações;
3.1.4.18. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch;
3.1.4.19. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’;
3.1.4.20. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”;
3.1.4.21. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft;
3.1.4.22. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários;
3.1.4.23. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes;
3.1.4.24. A solução proposta deve apoiar a implantação do sistema operacional;
3.1.4.25. A solução proposta deve suportar Wake-on LAN e UEFI;
3.1.4.26. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessãodevem ser registradas no Management Server;
3.1.4.27. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações;
3.1.4.28. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador;
3.1.4.29. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente;
3.1.4.30. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros;

3.1.4.31. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas;

3.1.4.32. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota;
3.1.4.33. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis;

3.1.4.34. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros;
3.1.4.35. A solução proposta deve permitir que o administrador configure regras para instalação depatches/atualizações da Microsoft e de terceiros:
3.1.4.35.1. Inicie a instalação ao reiniciar ou desligar o computador;

3.1.4.35.2. Instale o gerador necessário todos os pré-requisitos do

sistema;

3.1.4.35.3. Permitir a instalação de novas versões de aplicativos durante as

atualizações;3.1.4.35.4. Baixe atualizações para o dispositivo sem instalá-las;

3.1.4.36. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas;
3.1.4.37. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas deaplicativos e sistemas operacionais;
3.1.4.38. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs paraservidores SIEMs e SYSLOG nos seguintes formatos:
3.1.4.38.1. CEF;
3.1.4.38.2. LEEF;
3.1.4.39. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerarnotificações de quaisquer violações potenciais;
3.1.4.40. O relatório da solução proposta deve conter informações CVE;
3.1.4.41. A solução proposta deve suportar instalação de aplicações e software de

terceiros;3.1.5.Do módulo de gerenciamento simplificado

3.1.5.1. A solução proposta deve suportar arquitetura cloud;
3.1.5.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional;
3.1.5.3. O console de gerenciamento web da solução proposta deve ser simples de usar e devesuportar dispositivos com tela sensível ao toque;
3.1.5.4. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos;

3.1.5.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint;

3.1.5.6. A solução proposta deve atender as condições apontadas no item e subintes

3.1.6; 3.1.5.7. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS;

3.1.5.8. A solução proposta deve incluir informações do endpoint:
3.1.5.8.1. IP público de internet;
3.1.5.8.2. IP interno do dispositivo;

3.1.5.8.3. Versão do agente de proteção;
3.1.5.8.4. Última comunicação com a console, contendo data e hora;
3.1.5.8.5. Informações do sistema operacional;
3.1.5.9. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365 ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;
3.1.5.10. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365 ou compor com ferramenta do mesmo fabricanteque tenha capacidade similar;
3.1.5.11. A solução proposta deve incluir uma plataforma de capacitação online em segurança cibernética ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;
3.1.6. A solução proposta deve prover as seguintes proteções ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;
3.1.6.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
3.1.6.1.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados;
3.1.6.2. A solução proposta deve ser de um único fornecedor e suportar todos os módulos descritos neste termo de referência;
3.1.6.3. A solução proposta deve suportar integração com AntiMalware Scan Interface (AMSI);
3.1.6.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender;
3.1.6.5. A solução proposta deve suportar o subsistema Linux no Windows;
3.1.6.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
3.1.6.6.1. Proteção contra ameaças sem arquivos (Fileless);
3.1.6.7. Fornecimento de proteção baseada em machine learning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

3.1.6.8. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
3.1.6.9. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
3.1.6.10. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados;
3.1.6.11. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra

- ataques remotos de criptografia;

3.1.6.12. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para préexecução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows;
3.1.6.13. A solução proposta deve fornecer análise comportamental baseada em machine learning;
3.1.6.14. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento;
3.1.6.15. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
3.1.6.15.1. Controles de aplicativos;

3.1.6.15.2. Controle web e

dispositivos;3.1.6.15.3. HIPS e

Firewall;

3.1.6.15.4. Descoberta de patches e vulnerabilidades de sistemas operacionais

Windows;3.1.6.15.5. Gerenciamento de criptografia de arquivos e discos;

3.1.6.15.6. Controle adaptativo para detecção de anomalias;

3.1.6.16. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividadessemelhantes à criptografia em recursos compartilhados do servidor;
3.1.6.17. A solução proposta deve ser protegida por senha para evitar que o processo do AntiMalware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema;
3.1.6.18. A solução proposta deve ter bancos de dados de reputação locais e globais;
3.1.6.19. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTPcontra malwares;
3.1.6.20. A solução proposta deve incluir um módulo capaz, no mínimo,

de:3.1.6.20.1. Bloqueio de aplicativos com base em sua categorização;

3.1.6.20.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos;

3.1.6.20.3. A adição de sub-redes e a modificação de permissões de atividade;
3.1.6.21. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização;
3.1.6.22. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção;
3.1.6.23. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça;
3.1.6.24. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
3.1.6.24.1. Modo silencioso;
3.1.6.24.2. Discos rígidos e dispositivos removíveis;

3.1.6.24.3. De todas as contas de usuários do

dispositivo;

3.1.6.25. A funcionalidade de limpeza remota de dados da solução proposta deve suportar osseguintes modos:
3.1.6.25.1. Exclusão imediata de

dados;3.1.6.25.2. Exclusão de dados

adiada.

3.1.6.26. A funcionalidade de limpeza remota de dados da solução proposta deve suportar osseguintes métodos de exclusão de dados:
3.1.6.26.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
3.1.6.26.2. Excluir completamente, sem recuperação - tornando praticamente impossível restauraros dados após a exclusão.
3.1.6.27. A solução proposta deve ter uma abordagem proativa para impedir que malware explorevulnerabilidades existentes em servidores e estações de trabalho.
3.1.6.28. A solução proposta deve suportar a tecnologia AM-PPL (AntiMalware Protected Process Light) para proteção contra ações maliciosas;
3.1.6.29. A solução proposta deve incluir proteção contra-ataques que explorem vulnerabilidades noprotocolo ARP para falsificar o endereço MAC do dispositivo;

3.1.6.30. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário;
3.1.6.31. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem;

3.1.6.32. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas;

3.1.6.33. A solução proposta deve ser capaz de descriptografar e verificar o tráfego de rede transmitido por conexões criptografadas;
3.1.6.34. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
3.1.6.35. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
3.1.6.36. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint;
3.1.6.37. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem;
3.1.6.38. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada;
3.1.6.39. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas

dos computadores da rede de uma empresa;
3.1.6.40. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior;
3.1.6.41. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos

/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou duranteverificações sob demanda;

3.1.6.42. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint;
3.1.6.43. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos ou compor ferramenta do mesmo fabricante que tenha capacidade similar;
3.1.6.44. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos;
3.1.6.45. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo;
3.1.6.46. A solução proposta deve ter categoria de detecção para bloquear banners de sites;
3.1.6.47. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis ou compor ferramenta do mesmo fabricante que tenha capacidade similar;
3.1.6.48. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos;

3.1.6.49. A solução proposta deve apresentar integração na nuvem, para fornecer atualizaçõesmais rápidas possíveis sobre malware e ameaças potenciais;

3.1.6.50. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP ou compor ferramenta do mesmo fabricante que tenha capacidade similar;
3.1.6.51. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;
3.1.6.52. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações)de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aquelesincluídos nas listas de permissões;
3.1.6.53. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos;
3.1.6.54. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links daweb e controle de recursos da web com base em categorias de nuvem;
3.1.6.55. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração;
3.1.6.56. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões;
3.1.6.57. A solução proposta deve suportar o controle de scripts executados em PowerShell;
3.1.6.58. A solução proposta deve suportar modo teste com geração de relatórios sobre execuçãode aplicativos bloqueados;
3.1.6.59. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo;
3.1.6.60. A solução proposta deve fornecer um recurso para verificar os aplicativos listados

emcada categoria baseada em nuvem;
3.1.6.61. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor;
3.1.6.62. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas;
3.1.6.63. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint;
3.1.6.64. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint ou compor ferramenta do mesmo fabricante que tenha capacidade similar com:
3.1.6.64.1. Filtro de anexos;
3.1.6.64.2. Verificação de mensagens de e-mail ao receber, ler e enviar;
3.1.6.65. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo;
3.1.6.66. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

3.1.6.67. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (Javascript, Visual Basic Script Scripts WSH (Javascript, Visual Basic Script etc.);
3.1.6.68. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamentecom mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware;
3.1.6.69. A solução proposta deve fornecer proteção contra-ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio;
3.1.6.70. A solução proposta deve incluir suporte ao protocolo IPv6;
3.1.6.71. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente;
3.1.6.72. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

3.1.6.72.1. Protegendo contra o gerenciamento remoto não autorizado de um serviço de

aplicativo;

3.1.6.72.2. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando adesativação da proteção por malware, criminosos ou usuários;

3.1.6.73. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar;
3.1.6.74. A solução proposta deve incluir a verificação AntiMalware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha;
3.1.6.75. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística;
3.1.6.76. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail;
3.1.6.77. A solução proposta deve permitir ao administrador criar um único pacote de instalação dosensor de proteção com a configuração necessária;
3.1.6.78. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações detrabalho Windows;

3.1.6.79. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados;
3.1.6.80. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia, bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça;
3.1.6.81. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft;
3.1.6.82. A solução proposta deve suportar a instalação de proteção de endpoint em servidoressem a necessidade de reinicialização;

3.1.6.83. A solução proposta deve permitir a instalação de software com funcionalidades de AntiMalware e detecção e resposta de incidente a partir de um único pacote de distribuição;
3.1.6.84. A solução proposta deve suportar endereços IPv6;
3.1.6.85. A solução proposta deve suportar verificação em duas etapas (autenticação);
3.1.6.86. A solução proposta deve prever a instalação, atualização e remoção centralizada de software AntiMalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento;

3.1.6.87. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração;
3.1.6.88. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente;
3.1.6.89. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados AntiMalware mais recentes;
3.1.6.90. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de AntiMalware;
3.1.6.91. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas;
3.1.6.92. A solução proposta deve permitir a gestão de um componente que proíba a instalação e

/ou execução de programas;

3.1.6.93. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos;
3.1.6.94. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet;
3.1.6.95. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi, Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor;
3.1.6.96. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes;
3.1.6.97. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS;
3.1.6.98. A solução proposta deve proporcionar a administração centralizada de armazenamentosde backup e quarentena em todos os recursos da rede onde o sensor de endpoint está instalado;
3.1.6.99. A solução proposta deve prever a criação de contas internas para autenticar

administradores no servidor de administração;
3.1.6.100. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos;
3.1.6.101. A solução proposta deve ter a capacidade de excluir atualizações baixadas;

3.1.6.102. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados;
3.1.6.103. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português;
3.1.6.104. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints;
3.1.6.105. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos;
3.1.6.106. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou;
3.1.6.107. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor;
3.1.6.108. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional;
3.1.6.109. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor;

3.1.6.110. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
3.1.6.111. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível;
3.1.6.112. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica;
3.1.6.113. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados;
3.1.6.114. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado;

3.1.7. Do modulo de gerenciamento de dispositivos móveis
3.1.7.1. O modulo deve ser integrado a console de gerenciamento;
3.1.7.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
3.1.7.2.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition);
3.1.7.3. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
3.1.7.3.1. iOS 10–17 ou IPadOS 13–17;
3.1.7.4. A solução proposta deve oferecer suporte a dispositivos Android Device Owner;
3.1.7.5. A solução proposta deve suportar dispositivos iOS supervisionados;

3.1.7.6. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador;

3.1.7.7. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras;
3.1.7.8. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões;
3.1.7.9. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais);
3.1.7.10. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário;
3.1.7.11. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps;
3.1.7.12. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado;
3.1.7.13. A solução proposta deve ter recursos de conteinerização para dispositivos Android;
3.1.7.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dosdispositivos Android:
3.1.7.14.1. Dados em contêineres;

3.1.7.14.2. Contas de e-mail

corporativo;

3.1.7.14.3. Configurações para conexão à rede Wi-Fi corporativa e

VPN;3.1.7.14.4. Nome do ponto de acesso (APN);

3.1.7.14.5. Perfil do Android for

Wor;3.1.7.14.6. Recipiente KNOX;

3.1.7.14.7. Chave do gerenciador de licença KNOX;

3.1.7.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dosdispositivos iOS:
3.1.7.15.1. Todos os perfis de configuração

instalados;3.1.7.15.2. Todos os perfis de

provisionamento; 3.1.7.15.3. O perfil iOS MDM;

3.1.7.15.4. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas;

3.1.7.16. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo;
3.1.7.17. A solução proposta deve oferecer controles para garantir que todos os dispositivos

cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-senum conjunto de regras que deverá incluir as seguintes componentes:
3.1.7.17.1. Critérios de verificação do dispositivo;
3.1.7.17.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
3.1.7.18. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak etc.;
3.1.7.19. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
3.1.7.19.1. Cartões de memória e outras unidades

removíveis; 3.1.7.19.2. Câmera do dispositivo; 3.1.7.19.3.

Conexões Wi-Fi;

3.1.7.19.4. Conexões Bluetooth; 3.1.7.19.5. Porta de conexão

infravermelha;3.1.7.19.6. Ativação do ponto de acesso Wi-Fi;

3.1.7.19.7. Conexão de área de trabalho

remota;3.1.7.19.8. Sincronização de área de

trabalho;

3.1.7.19.9. Definir configurações da caixa de correio do

Exchange; 3.1.7.19.10. Configurar caixa de e-mail em

dispositivos iOS MDM; 3.1.7.19.11. Configure contêineres

Samsung KNOX;

3.1.7.19.12. Definir as configurações do perfil do Android for

Work;3.1.7.19.13. Configurar e-mail/calendário/contatos;

3.1.7.19.14. Defina as configurações de restrição de conteúdo de

mídia;3.1.7.19.15. Definir configurações de proxy no dispositivo

móvel; 3.1.7.19.16. Configurar certificados e SCEP;

3.1.7.20. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay;
3.1.7.21. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensormóvel:
3.1.7.21.1. Google Play, Huawei App Gallery e Apple App

Store;3.1.7.21.2. Portal de inscrição móvel KNOX;

3.1.7.21.3. Pacotes de instalação pré-configurados independentes;

3.1.7.22. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN)para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel;
3.1.7.23. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente;
3.1.7.24. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemasEMM de terceiros:
3.1.7.24.1. VMware AirWatch 9.3 ou posterior;
3.1.7.24.2. MobileIron 10.0 ou posterior;
3.1.7.24.3. IBM MaaS360 10.68 ou posterior;
3.1.7.24.4. Microsoft Intune 1908 ou posterior;
3.1.7.24.5. SOTI MobiControl 14.1.4 (1693) ou posterior;
3.1.7.25. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo;
3.1.7.26. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
3.1.7.26.1. Google Play; 3.1.7.26.2. Galeria de aplicativos

Huawei;3.1.7.26.3. Loja de aplicativos da Apple;

3.1.7.27. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo;

3.1.7.28. A solução proposta deve ser capaz de verificar programas instalados a partir da interfacedo dispositivo;
3.1.7.29. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário oude acordo com um agendamento;
3.1.7.30. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena;
3.1.7.31. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos;
3.1.7.32. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malwaree outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente;
3.1.7.33. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores;
3.1.7.34. A solução proposta deve fornecer funcionalidade Anti-roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente;
3.1.7.35. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel;
3.1.7.36. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis;

3.1.7.37. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel;
3.1.7.38. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido;

3.1.7.39. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
3.1.7.40. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

3.1.8. Do módulo de EDR

3.1.8.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta;
3.1.8.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados;
3.1.8.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
3.1.8.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
3.1.8.5. Deve apresentar informações detalhadas contendo:
3.1.8.5.1. Usuário que executou a ação;
3.1.8.5.2. Informações acesso privilegiado;
3.1.8.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas;
3.1.8.7. A solução proposta deve suportar integração com serviço de reputação em nuvem;
3.1.8.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações etc.);
3.1.8.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único);
3.1.8.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;

3.1.8.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem;
3.1.8.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção;
3.1.8.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta;
3.1.8.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados;

3.1.8.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador;
3.1.8.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede;
3.1.8.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores nãodetectadas; 3

3.1.8.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC;

3.1.8.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça

detectada em um endpoint;
3.1.8.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
3.1.8.20.1. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque);
3.1.8.20.2. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional;
3.1.8.20.3. Informações gerais sobre a detecção, incluindo modo de

detecção;3.1.8.20.4. Alterações no registro associadas à detecção;

3.1.8.20.5. Histórico da presença de arquivos no

dispositivo;3.1.8.20.6. Ações de resposta executadas

pela aplicação;

3.1.8.21. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.;
3.1.8.22. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistemae dos dados relacionados ao incidente para análise da causa raiz:
3.1.8.22.1. Processo;

3.1.8.22.2. Conexões de

rede;

3.1.8.22.3. Alterações no registro;

3.1.8.22.4. Detalhes do download de

objeto;

3.1.8.23. A solução proposta deve fornecer orientação de resposta (resposta guiada);
3.1.8.24. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente;
3.1.8.25. A solução proposta deve suportar pelo menos as seguintes ações de resposta que umadministrador pode executar quando ameaças são detectadas:
3.1.8.25.1. Impedir a execução de objetos

3.1.8.25.2. Isolamento de host
3.1.8.25.3. Excluir objeto do host ou grupo de

hosts3.1.8.25.4. Encerrar um processo no

dispositivo 3.1.8.25.5. Colocar um objeto em

quarentena 3.1.8.25.6. Execute a verificação do

sistema

3.1.8.25.7. Execução remota de

programa/processo/comando3.1.8.25.8. Iniciar a varredura

IoC para um grupo de hosts.

3.1.9. Requisitos para documentação da solução.

3.1.9.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
3.1.9.1.1. Ajuda on-line para administradores;
3.1.9.1.2. Ajuda on-line para melhores práticas de implementação;
3.1.9.1.3. Ajuda on-line para proteção de servidores de administração;
3.1.9.2. A documentação do software AntiMalware fornecida deve descrever detalhadamente osprocessos de instalação, configuração e uso do software AntiMalware;
3.1.9.3. Deve estar disponível página com informações de ciclo de vida das soluções e módulos.

3.1.10. Da Proteção para o Microsoft Office 365

3.1.10.1. Características Gerais ou compor ferramenta do mesmo fabricante que tenha capacidadesimilar;
3.1.10.1.1. A solução deve ser entregue no modelo de “Software as a Service”, onde servidor econsole administrativa são hospedados na nuvem;
3.1.10.1.2. Acesso a console administrativa via HTTPS;
3.1.10.1.3. A integração com o Office 365 deve ser realizada via API;
3.1.10.1.4. A autenticação da integração deve ser realizada via protocolo seguro OAuth 2.0;
3.1.10.1.5. A solução deve prover módulos de proteção para a suíte Microsoft Office 365 (ExchangeOnline, OneDrive, SharePoint e Teams);
3.1.10.1.6. A console deve prover painel de informações exibindo as informações principais daoperação e do estado dos componentes de proteção;

3.1.10.1.7. Capacidade de geração de relatórios em no mínimo formato

“.pdf”;3.1.10.1.8. Capacidade de geração de relatório instantâneo;

3.1.10.1.9. Capacidade de agendamento automático de relatórios;

3.1.10.1.10. A solução deve verificar o tráfego de e-mails inbound e

outbound;

3.1.10.1.11. Deve possuir quarentena para armazenar artefatos detectados como maliciosos;

3.1.10.1.12. A quarentena deve possuir no mínimo as seguintes

opções:3.1.10.1.12.1. Exibir detalhes do item;

3.1.10.1.12.2. Excluir item;
3.1.10.1.12.3. Liberar item;
3.1.10.1.12.4. Filtrar itens;

3.1.10.1.12.5. Salvar item em

disco;

3.1.10.1.13. A gestão da solução deve ser realizada por usuário com perfil de administrador;
3.1.10.1.14. Deve ser possível atribuir perfil de administrador para um usuário na console de administração;
3.1.10.1.15. Deve ser capaz de detectar informação sensível em texto e imagens transmitidos e armazenados através da plataforma e alertar o administrador quanto ao risco de vazamento da informação;

3.1.10.2. Módulo de Proteção - AntiMalware

3.1.10.2.1. Deve proteger as caixas de correio contra vírus, Worms, trojans, entre outras ameaçasque podem ser enviadas via e-mail.
3.1.10.2.2. Análise das ameaças deve ser realizada por no mínimo as seguintes

tecnologias:3.1.10.2.2.1. Assinaturas;

3.1.10.2.2.2. Heurística;
3.1.10.2.2.3. Comportamento;
3.1.10.2.2.4. Consulta ao repositório de inteligência do fabricante.

3.1.10.2.3. Capacidade de detectar ataques conhecidos e

desconhecidos.

3.1.10.2.4. Ao detectar um malware, a solução deve tomar uma ou mais ações de acordo com aconfiguração do administrador, possibilitando no mínimo:
3.1.10.2.4.1. Excluir a mensagem e colocá-la em quarentena;

3.1.10.2.4.2. Excluir anexo infectado e colocá-lo em

quarentena;3.1.10.2.4.3. Colocar tag no assunto;

3.1.10.2.4.4. Substituir arquivo por mensagem personalizada;

3.1.10.2.5. Notificar ao administrador sobre novas ameaças

encontradas;3.1.10.2.6. Notificar ao proprietário da caixa sobre

mensagens excluídas;3.1.10.2.7. Deve analisar arquivos nas

seguintes aplicações: 3.1.10.2.7.1. Exchange Online;

3.1.10.2.7.2. OneDrive;

3.1.10.2.7.3. SharePoint;

3.1.10.2.7.4. Teams;
3.1.10.2.8. Oferecer proteção contra-ataques mailsploit, ghost spoofing e injeções de código malicioso;

3.1.10.2.9. Módulo de Proteção – Anti-Phishing

3.1.10.2.9.1. Deve proteger as caixas de correio contra phishing e links maliciosos enviados em

mensagens de e-mail, evitando assim infecção por malware, roubo de dados pessoas e acesso a sites fraudulentos.
3.1.10.2.9.2. Deve validar o conteúdo das mensagens para detectar phishing, utilizando as seguintes tecnologias:
3.1.10.2.9.2.1. SPF (Sender Policy Framework);

3.1.10.2.9.2.2. DKIM (Domain-based Message

Authentication);

3.1.10.2.9.2.3.. DMARC (Domain-based Message Authentication, Reporting and

Conformance);3.1.10.2.9.2.4. Consulta ao repositório de inteligência do fabricante;

3.1.10.2.9.2.5. Capacidade de detectar ataques conhecidos e desconhecidos;

3.1.10.2.9.2.6.. Ao detectar um link de phishing, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:

3.1.10.2.9.2.7. Excluir a mensagem e colocá-la em

quarentena;3.1.10.2.9.2.8. Permitir;

3.1.10.2.9.2.9. Mover para pasta “Lixo

eletrônico”;3.1.10.2.9.2.10. Colocar tag no

assunto;

3.1.10.2.9.2.11. Notificar ao administrador sobre novas mensagens encontradas;

3.1.10.2.9.2.12. Notificar ao proprietário da caixa sobre mensagens excluídas;

3.1.10.2.9.2.13. Permitir a criação de exclusões por e-mail completo ou máscara.

3.1.10.3. Módulos de proteção - AntiSpam / Mass Mail
3.1.10.3.1. Deverá proteger todas as caixas de correio contra e-mail não solicitados “SPAM” e e-mails enviados em massa;
3.1.10.3.1.1. A verificação deve ser realizada através dos seguintes métodos:

3.1.10.3.1.2. Verificação de cabeçalho, conteúdo, anexos e elementos de

design;3.1.10.3.1.3. Algoritmos linguísticos e heurísticos;

3.1.10.3.1.4. Consulta ao repositório de inteligência do fabricante;

3.1.10.3.2. Ao detectar um SPAM, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:
3.1.10.3.2.1. Permitir;
3.1.10.3.2.2. Mover para a pasta “Lixo eletrônico”;

3.1.10.3.2.3. Colocar tag no assunto;
3.1.10.3.2.4. Notificar ao administrador sobre novas ameaças

encontradas; 3.1.10.3.2.5. Notificar ao proprietário da caixa sobre

mensagens excluídas; 3.1.10.3.2.6. Permitir a criação de exclusões por e-

mail completo ou máscara;

3.1.10.4. Módulo de proteção - Filtro de conteúdo
3.1.10.4.1. Deve possibilitar a filtragem de anexos em mensagens de e-

mail;3.1.10.4.2. Capacidade de detectar anexos pelos seguintes

parâmetros: 3.1.10.4.2.1. Formato do arquivo;

3.1.10.4.2.2. Nome completo do arquivo;

3.1.10.4.2.3. Nome do arquivo com

máscara;3.1.10.4.2.4. Arquivos MS Office

com macro;

3.1.10.4.3. Ao detectar um anexo que se encaixe em uma das regras, a solução deve possibilitar asseguintes ações:
3.1.10.4.3.1. Excluir mensagem e colocá-la em

quarentena;3.1.10.4.3.2. Excluir anexo e colocá-lo em

quarentena; 3.1.10.4.3.3. Permitir;

3.1.10.4.3.4. Colocar tag no assunto;
3.1.10.4.3.5. Substituir arquivo por mensagem personalizada;
3.1.10.4.3.6. Notificar ao administrador sobre novas ameaças

encontradas; 3.1.10.4.3.7. Notificar ao proprietário da caixa sobre

mensagens excluídas; 3.1.10.4.3.8. Permitir a criação de exclusões por e-

mail completo ou máscara.

ITEM 02 - SOFTWARE DE SEGURANÇA E ANTIVÍRUS PARA AMBIENTES VIRTUALIZADOSON PREMISE

3.1.11. Requerimentos para gerenciamento, administração e relatórios centralizados
3.1.11.1. Permitir a instalação de software AntiMalware a partir de um único pacote de distribuição;
3.1.11.2. Deve ter perfis de instalação personalizáveis dependendo do número de nós protegidos;
3.1.11.3. Suportar endereços IPv6.
3.1.11.4. Suportar verificação em duas etapas (autenticação);
3.1.11.5. Deve ter capacidade de ler informações do AD para obter dados sobre contas de computadores na organização;
3.1.11.6. Deverá incluir uma consola web incorporada para a gestão dos Endpoints, que não deveránecessitar de qualquer instalação adicional;

3.1.11.7. O console de gerenciamento web da solução proposta deve ser simples de usar e deve

suportar dispositivos de tela sensível ao toque;
3.1.11.8. Deve distribuir automaticamente as contas de computador por grupo de gerenciamento se novos computadores aparecerem na rede;
3.1.11.9. 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 AD;
3.1.11.10. Deverá prever a instalação, atualização e remoção centralizada de software AntiMalware, bem como configuração, administração e visualização centralizada de relatórios e informaçõesestatísticas sobre o seu funcionamento;
3.1.11.11. Deverá contemplar a remoção centralizada (manual e automática) de aplicativos incompatíveis do centro de administração;
3.1.11.12. Deverá 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;
3.1.11.13. Deverá permitir a instalação remota de software AntiMalware com as bases de dados AntiMalware mais recentes;
3.1.11.14. Deve permitir a atualização automática do software AntiMalware e das bases de dados AntiMalware;
3.1.11.15. Deve possibilitar o gerenciamento de um componente que proíba a instalação e/ou execução de programas;
3.1.11.16. Deve oferecer suporte à integração de API nativa com o Microsoft Azure e Google Cloud Platform;
3.1.11.17. Deve oferecer suporte à integração nativa da API com o ambiente de nuvem Amazon AWS, que inclui autenticação e localização de dispositivos usando a API AWS
3.1.11.18. Deve oferecer suporte à instalação remota de proteção usando API na AWS;
3.1.11.19. O servidor de gerenciamento centralizado da solução exibe recursos específicos da AWS (propriedades do dispositivo cliente, hierarquia de grupos de administração, Diretório AWS, assistente de configuração de proteção de segmento de nuvem e sondagem de segmento de nuvem) em sua interface;

3.1.11.20. Deve oferecer suporte a esquemas de licenciamento BYOL e PAYGo para proteção de nuvem pública;
3.1.11.21. Deve possibilitar o gerenciamento de um componente controlando o trabalho com dispositivos de E/S externos;
3.1.11.22. Deve possibilitar o gerenciamento de um componente que controla a atividade do usuário na internet;
3.1.11.23. 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;

3.1.11.24. 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;
3.1.11.25. 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;
3.1.11.26. 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;
3.1.11.27. Deve dar acesso aos serviços de nuvem do fornecedor de segurança AntiMalware por meio do servidor de administração;
3.1.11.28. Deve incluir a distribuição automática de licenças nos computadores clientes;
3.1.11.29. Deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários;

3.1.11.30. Deve ter um mecanismo de notificação para informar os usuários sobre eventos no software AntiMalware instalado e nas configurações, e para distribuir notificações sobre eventos via e-mail;
3.1.11.31. Permitir a instalação centralizada de aplicativos de terceiros em todos ou em alguns computadores;
3.1.11.32. 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.
3.1.11.33. Capacidade de especificar qualquer computador da organização como um centro de encaminhamento de eventos do agente AntiMalware 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;
3.1.11.34. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software AntiMalware, e dados sobre o inventário de hardware e software, licenciamento, etc.;
3.1.11.35. Deve ser capaz de exportar relatórios para arquivos PDF e XML;
3.1.11.36. Deve fornecer a administração centralizada de armazenamentos de backup e quarentena em todos os recursos de rede onde o software AntiMalware está instalado;
3.1.11.37. Deve prever a criação de contas internas para autenticar administradores no servidor de administração;
3.1.11.38. Deve prever a criação de uma cópia de backup do sistema de administração com o auxílio de ferramentas integradas do sistema de administração;
3.1.11.39. Deve oferecer suporte ao Windows Failover Cluster ou compor com outra solução de alta disponibilidade;
3.1.11.40. Deve ter um recurso de cluster integrado;
3.1.11.41. Deve incluir alguma forma de sistema para controlar epidemias de vírus;

3.1.11.42. Deve incluir Controle de Acesso Baseado em Função (RBAC), e isso deve permitir queas restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia;
3.1.11.43. O servidor de gerenciamento da solução deve incluir funções de segurança pré-definidas para Auditor, Supervisor e Agente de Segurança;
3.1.11.44. Capacidade de gerenciar dispositivos móveis por meio de comandos remotos;
3.1.11.45. Capacidade de excluir as atualizações baixadas;
3.1.11.46. Deve gerar atualizações do Servidor de Administração de Gerenciamento a partir da interface do aplicativo;
3.1.11.47. Deve permitir a seleção de um agente de atualização para computadores clientes com base em uma análise de rede;

3.1.11.48. O servidor de gerenciamento da solução 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;
3.1.11.49. O servidor de gerenciamento da solução 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:

3.1.11.49.1. Status do

dispositivo;3.1.11.49.2. Tag;

3.1.11.49.3. Diretório ativo;
3.1.11.49.4. Proprietários de

dispositivos;3.1.11.49.5. Hardware;

3.1.11.50. Suportar os seguintes canais de entrega de notificação:
3.1.11.50.1. E-mail;
3.1.11.50.2. Syslog;
3.1.11.51. Capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego docliente para o servidor de gestão com base no tempo e na velocidade;
3.1.11.52. Capacidade de realizar inventário em scripts e arquivos. arquivos dll;
3.1.11.53. Deve ter a capacidade de etiquetar/marcar computadores com base

em:3.1.11.53.1. Atributos de rede;

3.1.11.53.2. Nome;
3.1.11.53.3. Domínio e/ou Sufixo de

Domínio;3.1.11.53.4. IP;

3.1.11.53.5. Endereço IP para o servidor de

gerenciamento;3.1.11.53.6. Localização no Active

Directory;

3.1.11.53.7. Unidade organizacional;
3.1.11.53.8. Grupo;
3.1.11.53.9. Sistema

operacional;3.1.11.53.10. Tipo

e versão; 3.1.11.53.11.

Arquitetura;

3.1.11.53.12. Número do pacote de

serviço;3.1.11.53.13. Arquitetura virtual;

3.1.11.53.14. Registro de aplicativos;

3.1.11.53.15. Nome da Aplicação;

3.1.11.53.16. Versão do aplicativo;

3.1.11.53.17. Fabricante;

3.1.11.54. A solução deve ter a capacidade de criar/definir configurações com base na localizaçãode um computador na rede, e não no grupo ao qual pertence no servidor de gerenciamento;
3.1.11.55. Deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre oservidor de gerenciamento e o endpoint conectando pela internet/rede pública;
3.1.11.56. 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 definido. Os

valorespara o número de vírus e escala de tempo devem ser configuráveis;

3.1.11.57. Ter um painel personalizável gerando e exibindo estatísticas em tempo real para endpoints;
3.1.11.58. Deve permitir que o administrador personalize os relatórios;
3.1.11.59. Deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado;
3.1.11.60. Deve permitir que o administrador estabeleça um período após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados são excluídos automaticamente do servidor;
3.1.11.61. A solução deve permitir ao administrador criar categorias/grupos de aplicação com baseem:
3.1.11.61.1. Nome da Aplicação;

3.1.11.61.2. Caminho do Aplicativo;

3.1.11.61.3. Metadados do aplicativo;

3.1.11.61.4. Aplicativo certificado

digital;

3.1.11.61.5. Categorias de aplicativos pré-definidas pelo

fornecedor;3.1.11.61.6. SHA;

3.1.11.62. Computadores de referência para permitir/negar sua execução em endpoints;
3.1.11.63. Permitir que o administrador defina diferentes condições de alteração de status para grupos de endpoints no servidor de gerenciamento;
3.1.11.64. Permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento;
3.1.11.65. Deve ter um recurso/módulo embutido para coletar remotamente os dados necessários para solução de problemas dos endpoints, sem exigir acesso físico;
3.1.11.66. 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;
3.1.11.67. Deve ter funcionalidade integrada para se conectar remotamente ao ponto de extremidade usando a tecnologia de compartilhamento de área de trabalho do Windows. Alémdisso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão;

3.1.11.68. Deve possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:
3.1.11.68.1. Estruturas de domínios e grupos de trabalho do

Windows;3.1.11.68.2. Estruturas de grupos do AD;

3.1.11.68.3. Conteúdo de um arquivo de texto criado pelo administrador

manualmente;3.1.11.68.4. Ambiente AWS;

3.1.11.69. A solução deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa de rede. O inventário resultante deve abranger todos os equipamentosconectados à rede da organização;
3.1.11.70. As informações sobre o equipamento devem ser atualizadas após cada nova pesquisa de rede. A lista de equipamentos detectados deve abranger o seguinte:
3.1.11.70.1. Dispositivos;
3.1.11.70.2. Dispositivos

móveis; 3.1.11.70.3.

Dispositivos de rede;

3.1.11.70.4. Dispositivos

virtuais;

3.1.11.70.5. Componentes OEM;

3.1.11.70.6. Periféricos de

computador;3.1.11.70.7. Dispositivos

conectados;

3.1.11.70.8. Telefones VoIP;

3.1.11.70.9. Repositórios de rede;

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

3.1.11.72. A funcionalidade 'Device is Write Off' deve estar disponível, para que tais dispositivosnão sejam exibidos na lista de equipamentos;
3.1.11.73. A solução deve incorporar um único agente de distribuição/retransmissão para dar suporte a pelo menos 10.000 endpoints para a entrega de proteção, atualizações, patches e pacotes de instalação para sites remotos;
3.1.11.74. 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 degerenciamento;

3.1.11.75. Deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização;

3.1.11.76. Deve suportar OPEN API e incluir diretrizes para integração com sistemas externos de terceiros;
3.1.11.77. A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem a necessidade de acesso físico ao computador;
3.1.11.78. A solução proposta deve incluir Controle de Acesso Baseado em Função (RBAC) com funções predefinidas personalizáveis;

3.1.11.79. O servidor de gerenciamento primário/pai da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem;
3.1.11.80. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou;
3.1.11.81. O relatório da solução 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;
3.1.11.82. O servidor de gerenciamento principal deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade etc., dos terminais gerenciados dos servidores de gerenciamento secundário;
3.1.11.83. Deve incluir a opção para o cliente implantar um console de gerenciamento local ou usaro console de gerenciamento baseado em nuvem fornecido pelo fornecedor;
3.1.11.84. A solução deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional;
3.1.11.85. Deve permitir uma migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor;
3.1.11.86. Deve incluir a opção de integração SIEM – Syslog;
3.1.11.87. Deve incluir suporte para implantação baseada em nuvem por meio

de:3.1.11.87.1. Amazon Web Services;

3.1.11.87.2. Microsoft Azure;

3.1.11.88. Deve fornecer mecanismos de atualização de banco de dados AntiMalware, incluindo:
3.1.11.88.1. Múltiplas formas de atualização, incluindo canais de comunicação globais sobre o protocolo HTTPS, recurso compartilhado na rede local e mídia removível;

3.1.11.88.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica;
3.1.11.89. A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos;
3.1.12. Requisitos para antivírus em ambientes virtualizados baseado em agente para Windows;

3.1.12.1. Oferecer suporte aos seguintes sistemas operacionais:
3.1.12.1.1. Windows 11 21H2 Pro/ Enterprise/ Education;

3.1.12.1.2. Windows 10 Desktop Pro 19H1/19H2/20H1/20H2/21H1 (32 / 64-bit);

3.1.12.1.3. Windows 10 Enterprise 2016 LTSC/2019 LTSC/19H1/19H2/20H1/20H2/21H1 (32 / 64-

bit);

3.1.12.1.4. Windows 8.1 Update 1 Professional/Enterprise (32 / 64-bit);

3.1.12.1.5. Windows 7 Professional/Enterprise SP1 (32/64-bit);
3.1.12.1.6. Windows Server 2022 Standard/ Datacenter /Essentials (Desktop

experience/Core);3.1.12.1.7. Windows Server 2019 Standard/ Datacenter (Desktop

experience/Core);

3.1.12.1.8. Windows Server 2016 Standard/ Datacenter (Desktop experience/Core);

3.1.12.1.9. Windows Server 2012 R2 Standard/ Datacenter /Essentials (Desktop

experience/Core); 3.1.12.1.10. Windows Server 2012 Standard/ Datacenter /Essentials

(Desktop experience/Core); 3.1.12.1.11. Windows Server 2008 R2 SP1 Standard/Enterprise/

Datacenter (Desktop experience

/Core);

3.1.12.2. Características:
3.1.12.2.1. Oferecer suporte à verificação de objetos quando eles são

acessados;3.1.12.2.2. Suporte a verificações dos seguintes objetos:

3.1.12.2.2.1. Arquivos;
3.1.12.2.2.2. Fluxos alternativos do sistema de arquivos (fluxos NTFS);
3.1.12.2.2.3. Registro de inicialização e setores de inicialização em discos rígidos locais e unidades removíveis;
3.1.12.2.3. Suportar varredura sob demanda para executar 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;
3.1.12.2.4. 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;
3.1.12.2.5. Deve oferecer suporte a pastas compartilhadas de proteção em dispositivos contra criptografia maliciosa, bloqueando hosts que mostram atividade maliciosa;

3.1.12.2.6. Deve controlar a execução de scripts usando tecnologias de script do Microsoft Windows;
3.1.12.2.7. 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;
3.1.12.2.8. Deve verificar o tráfego de rede em busca de atividades típicas de ataques de rede e bloquear a atividade de rede do computador atacante;
3.1.12.2.9. 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;
3.1.12.2.10. 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;
3.1.12.2.11. 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;
3.1.12.2.12. Armazenar cópias criptografadas de objetos classificados como infectados no backup antes de desinfetá-los ou excluí-los;
3.1.12.2.13. Oferecer suporte a notificações do usuário;

3.1.12.2.14. Oferecer suporte à importação e exportação de configurações;
3.1.12.2.15. 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;
3.1.12.2.16. Deve oferecer suporte à proteção de memória contra explorações;
3.1.12.2.17. Deve suportar dispositivo de gerenciamento com a solução instalada via console de nuvem;
3.1.12.2.18. Fornecer integração com os mesmos fornecedores de Detecção de Endpoint e Resposta “EDR”, para busca ativa de ameaças e automação de resposta a incidentes;
3.1.13. Requisitos para antivírus em ambientes virtualizados baseado em agente para Linux;
3.1.13.1. A solução deve oferecer suporte aos seguintes sistemas

operacionais:3.1.13.1.1. CentOS 7.3 e posteriores (64-bit);

3.1.13.1.2. Debian GNU/Linux 9.4 e posteriores (32/64-

bit);3.1.13.1.3. Oracle Linux 7.3 e posteriores (64-bit);

3.1.13.1.4. Red Hat Enterprise Linux Server 7.3 e posteriores (64-

bit);3.1.13.1.5. SUSE Linux Enterprise Server 15 SP2 (64-bit);

3.1.13.1.6. Ubuntu 18.04 LTS e posteriores (64-bit);

3.1.13.2. Características:

3.1.13.2.1. Deve oferecer suporte a objetos do sistema de arquivos de varredura localizados nas unidades locais do computador, bem como recursos montados e compartilhados acessados pormeio dos protocolos SMB e NFS;
3.1.13.2.2. Oferecer suporte a varredura de objetos do sistema de arquivos em tempo real e sob demanda;
3.1.13.2.3. Deve oferecer suporte a digitalização de objetos de inicialização, setores de inicialização, processo e memória do kernel;
3.1.13.2.4. Suportar neutralizar ameaças detectadas em arquivos e escolher automaticamente qual ação executar para neutralizar a ameaça;
3.1.13.2.5. Oferecer suporte ao armazenamento de cópias de backup de arquivos antes da desinfecção ou exclusão e restauração de arquivos de cópias de backup;
3.1.13.2.6. Oferecer suporte à notificação do administrador sobre eventos ocorridos durante a operação;
3.1.13.2.7. 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;
3.1.13.2.8. Suporte à adição de chaves, bem como à ativação usando códigos de

ativação;3.1.13.2.9. Suporte ao gerenciamento de um firewall do sistema operacional;

3.1.13.2.10. Suporte à proteção de seus arquivos nos diretórios locais com acesso à rede porprotocolos SMB/NFS contra criptografia maliciosa remota;
3.1.13.2.11. Suporte à verificação de tráfego por meio dos protocolos HTTP/HTTPS e FTP e verificar se os endereços da Web são maliciosos ou phishing;
3.1.13.2.12. 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;

3.1.13.2.13. Suporte ao gerenciamento de dispositivos conectados com limitações de tempo e usuário por meio do Samba Active Directory e do Microsoft AD;
3.1.13.2.14. Deve oferecer suporte à verificação de unidades removíveis quando elas estão conectadas a um computador;
3.1.13.2.15. Oferecer suporte à inspeção de tráfego de rede para atividades típicas de ataques derede. Deve ser capaz de operar no modo somente notificação;
3.1.13.2.16. Suportar a verificação da reputação do objeto no banco de dados de reputação global;
3.1.13.2.17. Permitir que usuários não root gerenciem as funções básicas do aplicativo usando a GUI;
3.1.13.2.18. Oferecer suporte ao gerenciamento usando os seguintes métodos:

3.1.13.2.18.1.Na linha de comando usando os comandos de controle de

aplicativos;

3.1.13.2.18.2.Via console de gerenciamento central (console baseado em MMC e console da

web);3.1.13.2.18.3.GUI local;

3.1.13.2.19. Deve suportar capacidade de detecção de comportamento. Deve ser capaz de operarno modo somente notificação;
3.1.13.2.20. Deve suportar o trabalho com o sistema de arquivos GlusterFS;
3.1.13.2.21. Deve suportar dispositivo de gerenciamento com a solução instalada via console denuvem;
3.1.13.2.22. Deve suportar verificação da memória do kernel;
3.1.13.2.23. Oferecer suporte à verificação da integridade dos componentes do

aplicativo;3.1.13.2.24. Oferecer suporte aos recursos de controle de inicialização do

aplicativo;

3.1.13.2.25. Deve ser capaz de obter informações sobre todos os arquivos de programas executáveis armazenados nos computadores;
3.1.13.2.26. Oferecer suporte à opção de gerenciamento baseado em perfil;

3.1.14. Requisitos para antivírus em ambientes virtualizados baseado em agente para datacenter;

3.1.14.1. A solução deve suportar a seguinte infraestrutura virtual:

3.1.14.1.1. Microsoft Windows Server 2012 R2 Hyper-V e

posteriores;3.1.14.1.2. Citrix 8.2 LTSR;

3.1.14.1.3. Hypervisor VMware ESXi 6.5 e posteriores;
3.1.14.1.4. Plataforma KVM: Hypervisor KVM com um dos seguintes sistemas

operacionais:3.1.14.1.4.1. Servidor Ubuntu 16.04 LTS ou posteriores;

3.1.14.1.4.2. Servidor Red Hat Enterprise Linux 7. 9;

3.1.14.1.4.3. CentOS 7.9;
3.1.14.1.5. Proxmox VE 6.3 e posteriores;

3.1.14.1.6. Hipervisor R-Virtualization 7.0.13;
3.1.14.1.7. HUAWEI FusionSphere;
3.1.14.1.8. HUAWEI FusionCompute CNA 8.0;
3.1.14.1.9. Hipervisor Nutanix AHV 5.19.1;
3.1.14.1.10. Lançamentos da plataforma OpenStack: Stein, Victoria, Wallaby ou Xena;
3.1.14.2. A solução deve suportar as seguintes soluções de

virtualização:3.1.14.2.1. Citrix Virtual Apps and Desktops 7 1912

LTSR;

3.1.14.2.2. Citrix XenApp e XenDesktop 7.15 LTSR;

3.1.14.2.3. Provisionamento Citrix 7 1912 LTSR;

3.1.14.2.4. Serviços de Provisionamento Citrix 7.15

LTSR;

3.1.14.2.5. VMware Horizon 8.2 (2103);
3.1.14.2.6. Volumes de aplicativos VMware (2103);
3.1.14.2.7. HUAWEI FusionAccess 8.0 e posterior;
3.1.14.3. Deve oferecer suporte aos seguintes sistemas operacionais:
3.1.14.3.1. Windows 11;
3.1.14.3.2. Windows 10; (32 / 64 bits);
3.1.14.3.3. Windows 8.1 Update 1 Professional/Enterprise (32/64

bits)3.1.14.3.4. Windows 7 Pro / Enterprise SP1 (32/64 bits);

3.1.14.3.5. Windows Server 2019 Standard/ Datacenter (64 bits);
3.1.14.3.6. Windows Server 2016 Standard/ Datacenter (64 bits);
3.1.14.3.7. Windows Server 2012 e 2021 R2 Standard / Datacenter / Essentials (64

bits);3.1.14.3.8. Windows Server 2008 R2 SP1 Standard / Enterprise / Datacenter

(64 bits); 3.1.14.3.9. Debian GNU/Linux 10.3 (32/64 bits);

3.1.14.3.10. Debian GNU/Linux 9.8 (64 bits);
3.1.14.3.11. Debian GNU/Linux 8.11 (64 bits);
3.1.14.3.12. Debian GNU/Linux 8.11 i386 (32 bits);
3.1.14.3.13. Servidor Ubuntu 16.04 LTS e posteriores (64 bits);
3.1.14.3.14. CentOS 6.10 e posteriores (64 bits);
3.1.14.3.15. Red Hat Enterprise Linux Server 6.10 e posteriores (64

bits);3.1.14.3.16. SUSE Linux Enterprise Server 15 (64 bits);

3.1.14.3.17. Oracle Linux 7.6 (64 bits);

3.1.14.4. Características:

3.1.14.4.1. Deve oferecer suporte ao monitoramento AntiMalware;

3.1.14.4.2. Deve ter um analisador heurístico para detectar e bloquear malware anteriormente desconhecido;

3.1.14.4.3. 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;

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

3.1.14.4.5. Técnicas de redundância, que permitem a reconexão do agente a qualquer máquina virtual segura dentro da infraestrutura sem qualquer (re)configuração manual;

3.1.14.4.6. A solução deve oferecer suporte à instalação remota do agente para Windows e Linux;

3.1.14.4.7. 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 apósa restauração do acesso;

3.1.14.4.8. 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;

3.1.14.4.9. 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 ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;

3.1.14.4.10. Deve oferecer suporte à proteção do tráfego da Web: verificação de objetos – incluindoo 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;

3.1.14.4.11. 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.

3.1.14.4.12. Oferecer suporte à proteção contra programas maliciosos ainda desconhecidos com base em seu comportamento;

3.1.14.4.13. 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;

3.1.14.4.14. 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;

3.1.14.4.15. 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);

3.1.14.4.16. 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;

3.1.14.4.17. 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;

3.1.14.4.18. 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;

3.1.14.4.19. Deve armazenar as atualizações do banco de dados AntiMalware em máquinas virtuais seguras;

3.1.14.4.20. Permitir que os administradores instalem e distribuam remotamente componentes de software AntiMalware em todas as máquinas virtuais protegidas sem usar ferramentas de terceiros;

3.1.14.4.21. Deve oferecer suporte à verificação programada de todas as máquinas virtuais;

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

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

3.1.14.4.24. 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;

3.1.14.4.25. 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;

3.1.14.4.26. 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;

3.1.14.4.27. Deve fornecer informações detalhadas sobre eventos em máquinas virtuais e execução de tarefas de proteção;

3.1.14.4.28. Deve oferecer suporte à verificação de mensagens de e-mail recebidas e enviadas em busca de vírus e outros malwares;

3.1.14.4.29. Deve permitir que os administradores apliquem diferentes configurações de

segurançapara diferentes grupos de máquinas virtuais.

3.1.14.4.30. Deve oferecer suporte ao armazenamento de cópias de backup de arquivos

excluídos.3.1.14.4.31. Deve suportar a tecnologia VMware: vMotion, DRS;

3.1.14.4.32. Deve oferecer suporte para reversão de bancos de dados de antivírus;

3.1.14.4.33. Deve suportar um esquema de licenciamento de acordo com o número total de CPUsfísicas de cada host/hipervisor;

3.1.14.4.34. Oferecer suporte à proteção de máquinas virtuais que executam os sistemas operacionais Windows e Linux;

3.1.14.4.35. Oferecer suporte ao console de administração unificado para implantação e gerenciamento eficientes de toda a infraestrutura de segurança de TI;

3.1.14.4.36. 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;

3.1.14.4.37. 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;

3.1.14.4.38. Deve ter proteção de rede integrada, que detecta e bloqueia ataques diretos à rede;

3.1.14.4.39. A solução deve oferecer suporte à proteção da Web integrada, que detecta e bloqueiaURLs maliciosos;

3.1.14.4.40. Verifica todos os arquivos durante a verificação AntiMalware (mesmo arquivos maioresque 30 Mb);

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

3.1.14.4.42. Deve ter uma política de segurança para gerenciar todos os módulos de

proteção;3.1.14.4.43. Deve ser compatível com NSX Security Tags;

3.1.14.4.44. Deve oferecer suporte à proteção de pastas compartilhadas contra criptografia remota;

3.1.14.4.45. Deve oferecer suporte para ativação usando um código de ativação fornecido na assinatura;

3.1.14.4.46. Deve oferecer suporte à verificação de conexões seguras estabelecidas usando osprotocolos SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 ou TLS 1.3;

3.1.14.4.47. 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;

3.1.14.4.48. Deve oferecer suporte para o sistema de arquivos GlusterFS em máquinas virtuais que tenham o agente para Linux instalado;

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

3.1.14.4.50. Deve fornecer a capacidade de automatizar a implantação e o uso do aplicativo no modo multilocação usando a API REST;

3.1.14.4.51. 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;

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

3.1.14.4.53. 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;

3.1.14.4.54. A solução deve fornecer recursos de integração com o serviço gerenciado de detecçãoe resposta do mesmo fornecedor;

3.1.15. Requisitos para antivírus em ambientes virtualizados sem agentes para datacenter;
3.1.15.1. A solução deve suportar a seguinte infraestrutura

virtual:3.1.15.1.1. VMware vSphere versões 8.0 e 7.0;

3.1.15.1.2. VMware ESXi 6.5 Atualização 3 ou posterior;
3.1.15.1.3. VMware vCenter Server 6.5 Atualização 3 ou posterior;
3.1.15.2. VMware NSX Manager de um dos seguintes tipos:
3.1.15.2.1. NSX-V Manager do pacote VMware NSX Data Center para vSphere 6.4.10;
3.1.15.2.2. 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;
3.1.15.2.3. 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;
3.1.15.2.4. VMware vCloud Director 9.7.0.3 para provedores de serviços;

3.1.15.2.5. VMware vCloud Diretor versões 10.4, 10.3.3.2, 10.3.2.1, 10.3.0,

10.1.2;

3.1.15.3. A solução deve oferecer suporte aos seguintes sistemas

operacionais:3.1.15.3.1. Windows 10

3.1.15.3.2. Windows 8.1;
3.1.15.3.3. Windows 8;
3.1.15.3.4. Windows 7 SP1;
3.1.15.3.5. Windows Server 2019;
3.1.15.3.6. Windows Server 2016;
3.1.15.3.7. Windows Server 2012 e 2012 R2 sem suporte a ReFS;
3.1.15.3.8. Windows Server 2008 R2 SP1; 3.1.15.3.9. Ubuntu Server 14.04 GA e posteriores (64bits);

3.1.15.3.10. Red Hat Enterprise Linux Server 7.0 GA e posteriores (64

bits);3.1.15.3.11. SUSE Linux Enterprise Server 12 GA (64 bits);

3.1.15.3.12. CentOS 7.0 GA e posteriores (64 bits);

3.1.15.4. Características:
3.1.15.4.1. Oferecer suporte à proteção contra malware em tempo real e durante a verificaçãoagendada sem instalar um agente antivírus nas máquinas virtuais convidadas;
3.1.15.4.2. 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;

3.1.15.4.3. 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;
3.1.15.4.4. Suportar atualizações centralizadas na máquina de proteção especializada sem a necessidade de distribuir atualizações para cada máquina convidada;
3.1.15.4.5. Suporte à verificação sob demanda (ou manual) de máquinas virtuais

selecionadas; 3.1.15.4.6. Oferecer suporte à verificação de arquivos, pastas ou de todo o

sistema selecionados;3.1.15.4.7. Suporte à verificação programada de todas as máquinas

virtuais;

3.1.15.4.8. Fornecer a capacidade de implantar uma solução sem reinicialização do hipervisor ou modo de manutenção;
3.1.15.4.9. A solução não deve exigir uma nova verificação dos arquivos;
3.1.15.4.10. Deve impedir a nova verificação do mesmo objeto em diferentes máquinas convidadas em um único host;
3.1.15.4.11. Deve suportar bloqueio, neutralização e remoção de malware, notificação de administradores;
3.1.15.4.12. Deve permitir que os administradores vejam a estrutura de administração física e lógica conforme ela é apresentada no VMware vCenter;
3.1.15.4.13. Deve fornecer ao administrador informações detalhadas sobre eventos em máquinas virtuais e a implementação de tarefas;
3.1.15.4.14. Deve permitir que os administradores apliquem diferentes configurações de segurança para diferentes grupos de máquinas virtuais;
3.1.15.4.15. 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;

3.1.15.4.16. Permitir que os administradores exportem/importem uma lista de exceções;
3.1.15.4.17. Deve incluir a lista de exceções frequentes compiladas de acordo com as recomendações da Microsoft;

3.1.15.4.18. Deve permitir que os administradores verifiquem as unidades de rede conectadas à máquina virtual protegida, se necessário; 3.1.15.4.19. Permitir que os administradores excluam as unidades de rede da proteção;
3.1.15.4.20. Deve oferecer suporte para VMware vMotion e DRS;

3.1.15.4.21. Oferecer suporte ao armazenamento de cópias de backup de arquivos excluídos;

3.1.15.4.22. Deve suportar um esquema de licenciamento de acordo com o número total de CPUs físicas de cada host/hipervisor;

3.1.15.4.23. 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;

3.1.15.4.24. A solução deve oferecer suporte para ativação usando um código de ativação fornecidona assinatura;

3.1.15.4.25. Deve fornecer informações sobre o número de objetos verificados;

3.1.15.4.26. Deve fornecer informações sobre os detalhes do banco de dados de

antivírus;

3.1.15.4.27. Deve oferecer suporte à verificação de certificados SSL para comunicação entre omecanismo AntiMalware, o servidor de gerenciamento e os componentes da infraestrutura VMware;

3.1.15.4.28. Deve permitir que os administradores importem ou exportem a lista de exclusões deverificação e proteção em tarefas de verificação e perfis de proteção;

3.1.15.4.29. Deve permitir que os administradores protejam as máquinas virtuais que executam os sistemas operacionais Windows e Linux;

3.1.15.4.30. 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;

3.1.15.4.31. Deve permitir que os administradores especifiquem diferentes ações para ameaças encontradas em máquinas virtuais ligadas e desligadas;

3.1.15.4.32. Oferecer suporte ao modo multilocação - uma infraestrutura gerenciada por um VMware vCloud Director;

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

3.1.15.4.34. 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;

3.1.15.4.35. Deve ser capaz de desbloquear ataques de rede bloqueados incorretamente (Falso Positivo) sem demora;

3.1.15.4.36. Deve incluir a capacidade de verificar endereços da Web em um banco de dados global de endereços de phishing;

3.1.15.4.37. Deve ser capaz de restringir o acesso para configuração com base em contas de usuário;

3.1.15.4.38. Deve ser capaz de verificar máquinas virtuais Linux desligadas com os seguintes sistemas de arquivos: EXT2, EXT3, EXT4, XFS, BTRFS;

3.1.15.4.39. Deve ser capaz de digitalizar modelos de máquina virtual;

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

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

3.1.15.4.42. A solução deve suportar ambiente de grande escala;

ITEM 03 - SOFTWARE DE SEGURANÇA E ANTIVÍRUS PARA AMBIENTES VIRTUALIZADOSEM CLOUD

3.1.16. Requerimentos para gerenciamento, administração e relatórios centralizados

3.1.16.1. Permitir a instalação de software AntiMalware a partir de um único pacote de distribuição;

3.1.16.2. Deve ter perfis de instalação personalizáveis dependendo do número de nós protegidos;

3.1.16.3. Suportar endereços IPv6.

3.1.16.4. Suportar verificação em duas etapas (autenticação);

3.1.16.5.

3.1.16.6. Deve ter capacidade de ler informações do AD para obter dados sobre contas de computadores na organização;

3.1.16.7. Deverá incluir uma consola web incorporada para a gestão dos endpoints, que não deverá necessitar de qualquer instalação adicional;

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

3.1.16.9. Deve distribuir automaticamente as contas de computador por grupo de gerenciamento se novos computadores aparecerem na rede;

3.1.16.10. 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 AD;

3.1.16.11. Deverá prever a instalação, atualização e remoção centralizada de software AntiMalware, bem como configuração, administração e visualização centralizada de relatórios e informaçõesestatísticas sobre o seu funcionamento;

3.1.16.12. Deverá contemplar a remoção centralizada (manual e automática) de aplicativos incompatíveis do centro de administração;

3.1.16.13. Deverá 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;

3.1.16.14. Deverá permitir a instalação remota de software AntiMalware com as bases de dados AntiMalware mais recentes;

3.1.16.15. Deve permitir a atualização automática do software AntiMalware e das bases de dados AntiMalware;

3.1.16.16. Deve possibilitar o gerenciamento de um componente que proíba a instalação e/ou execução de programas;

3.1.16.17. Deve oferecer suporte à integração de API nativa com o Microsoft Azure e Google Cloud Platform;

3.1.16.18. Deve oferecer suporte à integração nativa da API com o ambiente de nuvem Amazon AWS, que inclui autenticação e localização de dispositivos usando a API AWS

3.1.16.19. Deve oferecer suporte à instalação remota de proteção usando API na AWS;

3.1.16.20. O servidor de gerenciamento centralizado da solução exibe recursos específicos da AWS (propriedades do dispositivo cliente, hierarquia de grupos de administração, Diretório AWS, assistente de configuração de proteção de segmento de nuvem e sondagem de segmento de nuvem) em sua interface;

3.1.16.21. Deve oferecer suporte a esquemas de licenciamento BYOL e PAYGo para proteção de nuvem pública;

3.1.16.22. Deve possibilitar o gerenciamento de um componente controlando o trabalho com dispositivos de E/S externos;

3.1.16.23. Deve possibilitar o gerenciamento de um componente que controla a atividade do

usuário na internet;

3.1.16.24. 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;

3.1.16.25. 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;

3.1.16.26. 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;

3.1.16.27. 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;

3.1.16.28. Deve dar acesso aos serviços de nuvem do fornecedor de segurança AntiMalware por meio do servidor de administração;

3.1.16.29. Deve incluir a distribuição automática de licenças nos computadores clientes;

3.1.16.30. Deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários;

3.1.16.31. Deve ter um mecanismo de notificação para informar os usuários sobre eventos no software AntiMalware instalado e nas configurações, e para distribuir notificações sobre eventos via e-mail;

3.1.16.32. Permitir a instalação centralizada de aplicativos de terceiros em todos ou em alguns computadores;

3.1.16.33. 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.

3.1.16.34. Capacidade de especificar qualquer computador da organização como um centro de encaminhamento de eventos do agente AntiMalware 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;

3.1.16.35. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software AntiMalware, e dados sobre o inventário de hardware e software, licenciamento, etc.;

3.1.16.36. Deve ser capaz de exportar relatórios para arquivos PDF e XML;

3.1.16.37. Deve fornecer a administração centralizada de armazenamentos de backup e quarentena em todos os recursos de rede onde o software AntiMalware está instalado;

3.1.16.38. Deve prever a criação de contas internas para autenticar administradores no servidor de administração;

3.1.16.39. Deve prever a criação de uma cópia de backup do sistema de administração com o auxílio de ferramentas integradas do sistema de administração;

3.1.16.40. Deve oferecer suporte ao Windows Failover Cluster ou compor com outra solução de alta disponibilidade; 3.1.16.40. Deve ter um recurso de cluster integrado;

3.1.16.41. Deve incluir alguma forma de sistema para controlar epidemias de vírus;

3.1.16.42. Deve incluir Controle de Acesso Baseado em Função (RBAC), e isso deve permitir queas restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia;

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

3.1.16.44. Capacidade de gerenciar dispositivos móveis por meio de comandos remotos; 3.1.16.45. Capacidade de excluir as atualizações baixadas;

3.1.16.46. Deve gerar atualizações do Servidor de Administração de Gerenciamento a partir da interface do aplicativo;

3.1.16.47. Deve permitir a seleção de um agente de atualização para computadores clientes com base em uma análise de rede;

3.1.16.48. O servidor de gerenciamento da solução 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;

3.1.16.49. O servidor de gerenciamento da solução 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:

3.1.16.49.1. Status do

dispositivo;3.1.16.49.2. Tag;

3.1.16.49.3. Diretório ativo;

3.1.16.49.4. Proprietários de

dispositivos;3.1.16.49.5. Hardware;

3.1.16.50. Suportar os seguintes canais de entrega de notificação:

3.1.16.50.1. E-mail;

3.1.16.50.2. Syslog;

3.1.16.51. Capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego docliente para o servidor de gestão com base no tempo e na velocidade;

3.1.16.52. Capacidade de realizar inventário em scripts e arquivos. arquivos dll;

3.1.16.53. Deve ter a capacidade de etiquetar/marcar computadores com base em:3.1.16.53.1. Atributos de rede;

3.1.16.53.2. Nome;

3.1.16.53.3. Domínio e/ou Sufixo de Domínio;3.1.16.53.4. IP;

3.1.16.53.5. Endereço IP para o servidor de gerenciamento;3.1.16.53.6. Localização no Active Directory;

Unidade organizacional;

3.1.16.53.7. Grupo;

3.1.16.53.8. Sistema operacional;3.1.16.53.10. Tipo e versão; 3.1.16.53.11. Arquitetura;

3.1.16.53.12. Número do pacote de serviço;3.1.16.53.13. Arquitetura virtual;

3.1.16.53.14. Registro de aplicativos;

3.1.16.53.15. Nome da Aplicação;

3.1.16.53.16. Versão do aplicativo;

3.1.16.53.17. Fabricante;

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

3.1.16.55. Deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre oservidor de gerenciamento e o endpoint conectando pela internet/rede pública;

3.1.16.56. 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 definido. Os valorespara o número de vírus e escala de tempo devem ser configuráveis;

3.1.16.57. Ter um painel personalizável gerando e exibindo estatísticas em tempo real para endpoints;

3.1.16.58. Deve permitir que o administrador personalize os relatórios;

3.1.16.59. Deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado;

3.1.16.60. Deve permitir que o administrador estabeleça um período após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados são excluídos automaticamente do servidor;

3.1.16.61. A solução deve permitir ao administrador criar categorias/grupos de aplicação com baseem:

3.1.16.61.1. Nome da Aplicação;

3.1.16.61.2. Caminho do Aplicativo;

3.1.16.61.3. Metadados do aplicativo;

3.1.16.61.4. Aplicativo certificado

digital;

3.1.16.61.5. Categorias de aplicativos pré-definidas pelo

fornecedor;3.1.16.61.6. SHA;

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

3.1.16.63. Permitir que o administrador defina diferentes condições de alteração de status para

grupos de endpoints no servidor de gerenciamento;

3.1.16.64. Permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento;

3.1.16.65. Deve ter um recurso/módulo embutido para coletar remotamente os dados necessários para solução de problemas dos endpoints, sem exigir acesso físico;

3.1.16.66. 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;

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

3.1.16.68. Deve possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

3.1.16.68.1. Estruturas de domínios e grupos de trabalho do

Windows;3.1.16.68.2. Estruturas de grupos do AD;

3.1.16.68.3. Conteúdo de um arquivo de texto criado pelo administrador

manualmente;3.1.16.68.4. Ambiente AWS;

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

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

3.1.16.70.1. Dispositivos;

3.1.16.70.2. Dispositivos

móveis; 3.1.16.70.3.

Dispositivos de rede;

3.1.16.70.4. Dispositivos

virtuais;

3.1.16.70.5. Componentes OEM;

3.1.16.70.6. Periféricos de

computador;3.1.16.70.7. Dispositivos

conectados;

3.1.16.70.8. Telefones VoIP;

3.1.16.70.9. Repositórios de rede;

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

3.1.16.72. A funcionalidade 'Device is Write Off' deve estar disponível, para que tais dispositivosnão sejam exibidos na lista de equipamentos;

3.1.16.73. A solução deve incorporar um único agente de distribuição/retransmissão para dar suporte a pelo menos 10.000 endpoints para a entrega de proteção, atualizações, patches e pacotes de instalação para sites remotos;

3.1.16.74. 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 degerenciamento;

3.1.16.75. Deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização;

3.1.16.76. Deve suportar OPEN API e incluir diretrizes para integração com sistemas externos de terceiros;

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

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

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

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

3.1.16.81. O relatório da solução 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;

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

3.1.16.83. Deve incluir a opção para o cliente implantar um console de gerenciamento local ou usaro console de gerenciamento baseado em nuvem fornecido pelo fornecedor;

3.1.16.84. A solução deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional;

3.1.16.85. Deve permitir uma migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor;

3.1.16.86. Deve incluir a opção de integração SIEM – Syslog;

3.1.16.87. Deve incluir suporte para implantação baseada em nuvem por meio

de:3.1.16.87.1. Amazon Web Services;

3.1.16.87.2. Microsoft Azure;

3.1.16.88. Deve fornecer mecanismos de atualização de banco de dados AntiMalware, incluindo:

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

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

3.1.16.89. A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos;

3.1.17. Requisitos para antivírus em ambientes virtualizados baseado em agente para Windows;

3.1.17.1. Oferecer suporte aos seguintes sistemas operacionais:

3.1.17.1.1. Windows 11 21H2 Pro/Enterprise/Education;

3.1.17.1.2. Windows 10 Desktop Pro 19H1/19H2/20H1/20H2/21H1 (32 / 64-bit);

3.1.17.1.3. Windows 10 Enterprise 2016 LTSC/2019 LTSC/19H1/19H2/20H1/20H2/21H1 (32 / 64-

bit);

3.1.17.1.4. Windows 8.1 Update 1 Professional/Enterprise (32 / 64-bit);

3.1.17.1.5. Windows 7 Professional/Enterprise SP1 (32/64-bit);

3.1.17.1.6. Windows Server 2022 Standard/ Datacenter /Essentials (Desktop experience/Core);3.1.17.1.7. Windows Server 2019 Standard/ Datacenter (Desktop experience/Core);

3.1.17.1.8. Windows Server 2016 Standard/ Datacenter (Desktop experience/Core);

3.1.17.1.9. Windows Server 2012 R2 Standard/ Datacenter /Essentials (Desktop experience/Core); 3.1.17.1.10. Windows Server 2012 Standard/ Datacenter /Essentials (Desktop experience/Core); 3.1.17.1.11. Windows Server 2008 R2 SP1 Standard/Enterprise/ Datacenter (Desktop experience /Core);

3.1.17.2. Características:

3.1.17.2.1. Oferecer suporte à verificação de objetos quando eles são acessados;3.1.17.2.2. Suporte a verificações dos seguintes objetos:

3.1.17.2.2.1. Arquivos;

3.1.17.2.2.2. Fluxos alternativos do sistema de arquivos (fluxos NTFS);

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

3.1.17.2.3. Suportar varredura sob demanda para executar 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;

3.1.17.2.4. 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;

3.1.17.2.5. Deve oferecer suporte a pastas compartilhadas de proteção em dispositivos contra criptografia maliciosa, bloqueando hosts que mostram atividade maliciosa;

3.1.17.2.6. Deve controlar a execução de scripts usando tecnologias de script do Microsoft Windows;

3.1.17.2.7. 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;

3.1.17.2.8. Deve verificar o tráfego de rede em busca de atividades típicas de ataques de rede e bloquear a atividade de rede do computador atacante;

3.1.17.2.9. 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;

3.1.17.2.10. 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;

3.1.17.2.11. 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;

3.1.17.2.12. Armazenar cópias criptografadas de objetos classificados como infectados no backup antes de desinfetá-los ou excluí-los;

3.1.17.2.13. Oferecer suporte a notificações do usuário;

3.1.17.2.14. Oferecer suporte à importação e exportação de configurações;

3.1.17.2.15. 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;

3.1.17.2.16. Deve oferecer suporte à proteção de memória contra explorações;

3.1.17.2.17. Deve suportar dispositivo de gerenciamento com a solução instalada via console de nuvem;

3.1.17.2.18. Fornecer integração com os mesmos fornecedores de Detecção de Endpoint e Resposta “EDR”, para busca ativa de ameaças e automação de resposta a incidentes;

3.1.18. Requisitos para antivírus em ambientes virtualizados baseado em agente para Linux;

3.1.18.1. A solução deve oferecer suporte aos seguintes sistemas

operacionais:3.1.18.1.1. CentOS 7.3 e posteriores (64-bit);

3.1.18.1.2. Debian GNU/Linux 9.4 e posteriores (32/64-

bit);3.1.18.1.3. Oracle Linux 7.3 e posteriores (64-bit);

3.1.18.1.4. Red Hat Enterprise Linux Server 7.3 e posteriores (64-

bit);3.1.18.1.5. SUSE Linux Enterprise Server 15 SP2 (64-bit);

3.1.18.1.6. Ubuntu 18.04 LTS e posteriores (64-bit);

3.1.18.2. Características:

3.1.18.2.1. Deve oferecer suporte a objetos do sistema de arquivos de varredura localizados nas unidades locais do computador, bem como recursos montados e compartilhados acessados pormeio dos protocolos SMB e NFS;

3.1.18.2.2. Oferecer suporte a varredura de objetos do sistema de arquivos em tempo real e sob demanda;

3.1.18.2.3. Deve oferecer suporte a digitalização de objetos de inicialização, setores de inicialização, processo e memória do kernel;

3.1.18.2.4. Suportar neutralizar ameaças detectadas em arquivos e escolher automaticamente qual ação executar para neutralizar a ameaça;

3.1.18.2.5. Oferecer suporte ao armazenamento de cópias de backup de arquivos antes da desinfecção ou exclusão e restauração de arquivos de cópias de backup;

3.1.18.2.6. Oferecer suporte à notificação do administrador sobre eventos ocorridos durante a operação;

3.1.18.2.7. 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;

3.1.18.2.8. Suporte à adição de chaves, bem como à ativação usando códigos de

ativação;3.1.18.2.9. Suporte ao gerenciamento de um firewall do sistema operacional;

3.1.18.2.10. Suporte à proteção de seus arquivos nos diretórios locais com acesso à rede porprotocolos SMB/NFS contra criptografia maliciosa remota;

3.1.18.2.11. Suporte à verificação de tráfego por meio dos protocolos HTTP/HTTPS e FTP e verificar se os endereços da Web são maliciosos ou phishing;

3.1.18.2.12. 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;

3.1.18.2.13. Suporte ao gerenciamento de dispositivos conectados com limitações de tempo e usuário por meio do Samba Active Directory e do Microsoft AD;

3.1.18.2.14. Deve oferecer suporte à verificação de unidades removíveis quando elas estão conectadas a um computador;

3.1.18.2.15. Oferecer suporte à inspeção de tráfego de rede para atividades típicas de ataques derede. Deve ser capaz de operar no modo somente notificação;

3.1.18.2.16. Suportar a verificação da reputação do objeto no banco de dados de reputação global;

3.1.18.2.17. Permitir que usuários não root gerenciem as funções básicas do aplicativo usando a GUI;

3.1.18.2.18. Oferecer suporte ao gerenciamento usando os seguintes métodos:

3.1.18.2.18.1.Na linha de comando usando os comandos de controle de

aplicativos;

3.1.18.2.18.2.Via console de gerenciamento central (console baseado em MMC e console da

web);3.1.18.2.18.3.GUI local;

3.1.18.2.19. Deve suportar capacidade de detecção de comportamento. Deve ser capaz de operarno modo somente notificação; 3.1.18.2.20. Deve suportar o trabalho com o sistema de arquivos GlusterFS;

3.1.18.2.21. Deve suportar dispositivo de gerenciamento com a solução instalada via console de nuvem;

3.1.18.2.22. Deve suportar verificação da memória do kernel;

3.1.18.2.23. Oferecer suporte à verificação da integridade dos componentes do

aplicativo;3.1.18.2.24. Oferecer suporte aos recursos de controle de inicialização do

aplicativo;

3.1.18.2.25. Deve ser capaz de obter informações sobre todos os arquivos de programas executáveis armazenados nos computadores;

3.1.18.2.26. Oferecer suporte à opção de gerenciamento baseado em perfil;

3.1.19. Requisitos para antivírus em ambientes virtualizados baseado em agente para datacenter;

3.1.19.1. A solução deve suportar a seguinte infraestrutura virtual:

3.1.19.1.1. Microsoft Windows Server 2012 R2 Hyper-V e

posteriores;3.1.19.1.2. Citrix 8.2 LTSR;

3.1.19.1.3. Hypervisor VMware ESXi 6.5 e posteriores;

3.1.19.1.4. Plataforma KVM: Hypervisor KVM com um dos seguintes sistemas

operacionais:3.1.19.1.4.1. Servidor Ubuntu 16.04 LTS ou posteriores;

3.1.19.1.4.2. Servidor Red Hat Enterprise Linux 7. 9;

3.1.19.1.4.3. CentOS 7.9;

3.1.19.1.5. Proxmox VE 6.3 e posteriores;

3.1.19.1.6. Hipervisor R-Virtualization 7.0.13;

3.1.19.1.7. HUAWEI FusionSphere;

3.1.19.1.8. HUAWEI FusionCompute CNA 8.0;

3.1.19.1.9. Hipervisor Nutanix AHV 5.19.1;

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

3.1.19.2. A solução deve suportar as seguintes soluções de

virtualização:3.1.19.2.1. Citrix Virtual Apps and Desktops 7 1912

LTSR;

3.1.19.2.2. Citrix XenApp e XenDesktop 7.15 LTSR;

3.1.19.2.3. Provisionamento Citrix 7 1912 LTSR;

3.1.19.2.4. Serviços de Provisionamento Citrix 7.15 LTSR;3.1.19.2.5. VMware Horizon 8.2 (2103);

3.1.19.2.6. Volumes de aplicativos VMware (2103);

3.1.19.2.7. HUAWEI FusionAccess 8.0 e posterior;

3.1.19.3. Deve oferecer suporte aos seguintes sistemas operacionais:

3.1.19.3.1. Windows 11;

3.1.19.3.2. Windows 10; (32 / 64 bits);

3.1.19.3.3. Windows 8.1 Update 1 Professional/Enterprise (32/64 bits)3.1.19.3.4. Windows 7 Pro / Enterprise SP1 (32/64 bits);

3.1.19.3.5. Windows Server 2019 Standard/ Datacenter (64 bits);

3.1.19.3.6. Windows Server 2016 Standard/ Datacenter (64 bits);

3.1.19.3.7. Windows Server 2012 e 2021 R2 Standard / Datacenter / Essentials (64 bits);3.1.19.3.8. Windows Server 2008 R2 SP1 Standard / Enterprise / Datacenter (64 bits); 3.1.19.3.9. Debian GNU/Linux 10.3 (32/64 bits);

3.1.19.3.10. Debian GNU/Linux 9.8 (64 bits);

3.1.19.3.11. Debian GNU/Linux 8.11 (64 bits);

3.1.19.3.12. Debian GNU/Linux 8.11 i386 (32 bits);

3.1.19.3.13. Servidor Ubuntu 16.04 LTS e posteriores (64 bits);

3.1.19.3.14. CentOS 6.10 e posteriores (64 bits);

3.1.19.3.15. Red Hat Enterprise Linux Server 6.10 e posteriores (64

bits);3.1.19.3.16. SUSE Linux Enterprise Server 15 (64 bits);

3.1.19.3.17. Oracle Linux 7.6 (64 bits); 3.1.19.4. Características:

3.1.19.4.1. Deve oferecer suporte ao monitoramento AntiMalware;

3.1.19.4.2. Deve ter um analisador heurístico para detectar e bloquear malware anteriormente desconhecido;

3.1.19.4.3. 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;

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

3.1.19.4.5. Técnicas de redundância, que permitem a reconexão do agente a qualquer máquina virtual segura dentro da infraestrutura sem qualquer (re)configuração manual;

3.1.19.4.6. A solução deve oferecer suporte à instalação remota do agente para Windows e Linux;

3.1.19.4.7. 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 apósa restauração do acesso;

3.1.19.4.8. 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;

3.1.19.4.9. 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, ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;

3.1.19.4.10. Deve oferecer suporte à proteção do tráfego da Web: verificação de objetos – incluindoo 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;

3.1.19.4.11. 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.

3.1.19.4.12. Oferecer suporte à proteção contra programas maliciosos ainda desconhecidos com base em seu comportamento;

3.1.19.4.13. 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;

3.1.19.4.14. 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;

3.1.19.4.15. 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);

3.1.19.4.16. 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;

3.1.19.4.17. 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;

3.1.19.4.18. 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;

3.1.19.4.19. Deve armazenar as atualizações do banco de dados AntiMalware em máquinas virtuais seguras;

3.1.19.4.20. Permitir que os administradores instalem e distribuam remotamente componentes de software AntiMalware em todas as máquinas virtuais protegidas sem usar ferramentas de terceiros;

3.1.19.4.21. Deve oferecer suporte à verificação programada de todas as máquinas virtuais;

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

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

3.1.19.4.24. 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;

3.1.19.4.25. 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;

3.1.19.4.26. 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;

3.1.19.4.27. Deve fornecer informações detalhadas sobre eventos em máquinas virtuais e execução de tarefas de proteção;

3.1.19.4.28. Deve oferecer suporte à verificação de mensagens de e-mail recebidas e enviadas em busca de vírus e outros malwares;

3.1.19.4.29. Deve permitir que os administradores apliquem diferentes configurações de segurançapara diferentes grupos de máquinas virtuais.

3.1.19.4.30. Deve oferecer suporte ao armazenamento de cópias de backup de arquivos

excluídos.3.1.19.4.31. Deve suportar a tecnologia VMware: vMotion, DRS;

3.1.19.4.32. Deve oferecer suporte para reversão de bancos de dados de antivírus;

3.1.19.4.33. Deve suportar um esquema de licenciamento de acordo com o número total de VM(virtual machines);

3.1.19.4.34. Oferecer suporte à proteção de máquinas virtuais que executam os sistemas operacionais Windows e Linux;

3.1.19.4.35. Oferecer suporte ao console de administração unificado para implantação e gerenciamento eficientes de toda a infraestrutura de segurança de TI;

3.1.19.4.36. 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;

3.1.19.4.37. 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;

3.1.19.4.38. Deve ter proteção de rede integrada, que detecta e bloqueia ataques diretos à rede;

3.1.19.4.39. A solução deve oferecer suporte à proteção da Web integrada, que detecta e bloqueiaURLs maliciosos;

3.1.19.4.40. Verifica todos os arquivos durante a verificação AntiMalware (mesmo arquivos maioresque 30 Mb);

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

3.1.19.4.42. Deve ter uma política de segurança para gerenciar todos os módulos de

proteção;3.1.19.4.43. Deve ser compatível com NSX Security Tags;

3.1.19.4.44. Deve oferecer suporte à proteção de pastas compartilhadas contra criptografia remota;

3.1.19.4.45. Deve oferecer suporte para ativação usando um código de ativação fornecido na assinatura;

3.1.19.4.46. Deve oferecer suporte à verificação de conexões seguras estabelecidas usando osprotocolos SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 ou TLS 1.3;

3.1.19.4.47. 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;

3.1.19.4.48. Deve oferecer suporte para o sistema de arquivos GlusterFS em máquinas virtuais que tenham o agente para Linux instalado;

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

3.1.19.4.50. Deve fornecer a capacidade de automatizar a implantação e o uso do aplicativo no modo multilocação usando a API REST;

3.1.19.4.51. 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;

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

3.1.19.4.53. 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;

3.1.19.4.54. A solução deve fornecer recursos de integração com o serviço gerenciado de detecçãoe resposta do mesmo fornecedor;

ITEM 04 – SOFTWARE DE COMPLEMENTO DE DETECÇÃO E RESPOSTA PARA OS ITENS 02 E 03

3.1.20. Deverá ser compatível com os seguintes sistemas operacionais:

3.1.20.1. Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

3.1.20.2. Microsoft Windows 8 Professional/Enterprise;

3.1.20.3. Microsoft Windows 8.1 Professional / Enterprise;

3.1.20.4. Microsoft Windows 10 Pro / Enterprise / Home / Education;

3.1.20.5. Microsoft Windows 11 Pro / Enterprise / Home / Education;

3.1.20.6. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

3.1.20.7. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

3.1.20.8. Windows Server 2016 Essentials / Standard / Datacenter;

3.1.20.9. Windows Server 2019 Essentials / Standard / Datacenter;

3.1.20.10. Windows Server 2022.

3.1.21. Das características do módulo de EDR:

3.1.21.1. As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;

3.1.21.2. A solução deve oferecer módulo focado em capacidades de EDR “Endpoint Detection and Response”, incluindo no mínimo as seguintes capacidades:

3.1.21.2.1. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito eao contexto da ameaça;

3.1.21.2.2. Deve fornecer graficamente a visualização da cadeia do ataque;

3.1.21.2.3. Deve possuir a capacidade de varredura, identificando a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).

3.1.21.3. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

3.1.21.3.1. Isolar o host;

3.1.21.3.2. Iniciar uma varredura nas áreas

críticas;3.1.21.3.3. Quarentenar o objeto;

3.1.21.4. A solução deve criar um relatório detalhado sobre o incidente, tendo a capacidade deincluir no mínimo os seguintes dados:

3.1.21.4.1. Visibilidade das detecções provenientes de

endpoint;3.1.21.4.2. Processos;

3.1.21.4.3. Conexões remotas;

3.1.21.4.4. Alterações de

registros;3.1.21.4.5. Objetos

baixados

3.1.21.4.6. Capacidade de integração com a solução de SandBox cloud do fabricante;

3.1.21.5. Varredura por todos os dispositivos executada a partir de indicador de comprometimento(IoC) gerado através da solução e importado pelo administrador;

3.1.21.6. Deverá possuir informações de assinaturas digitais da ameaça;

3.1.21.7. Deve ser capaz de trazer informações do arquivo sobre sua geolocalização;

3.1.21.8. Possibilidade de informar quando o arquivo foi detectado pela base de conhecimento;

3.1.21.9. Trazer a identificação de comportamento e/ou descrição sobre o arquivo;

3.1.21.10. A solução deve oferecer no mínimo as seguintes opções de

resposta:3.1.21.10.1. Prevenir a execução de um arquivo;

3.1.21.10.2. Quarentenar um arquivo;

3.1.21.10.3. Iniciar uma varredura por

IoC;3.1.21.10.4. Parar um processo;

3.1.21.10.5. Executar um processo;

3.1.21.11. Ferramenta que possibilite o isolamento do host infectado com no mínimo as

características abaixo:

3.1.21.11.1. A opção de isolamento deve estar disponível junto a visualização do

incidente;3.1.21.11.2. Deverá ser possível remover a máquina do isolamento a partir

do incidente;

3.1.21.11.3. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

3.1.21.12. Na análise do incidente a ferramenta deverá apresentar recomendações de ações necessárias para executar para remediar o incidente;

3.1.21.13. A recomendação deve ser guiada juntamente com guias das opções selecionadas peloanalista, apresentando pop-up guiando as ações.

3.1.21.14. Deverá oferecer informações de inteligência de ameaças do próprio fabricante;

3.1.21.15. Deverá possuir detecção baseada em sandbox do tipo cloud;

3.1.21.16. Deverá suportar IoC de terceiros em formatos OpenIOC.

ITEM 05 – SOFTWARE DE DETECÇÃO E RESPOSTA GERENCIADO

3.1.22. Do monitoramento, identificação e investigação dos eventos de segurança cibernética

3.1.22.1. O serviço de monitoramento deverá utilizar informações extraídas de registros geradospelos sistemas monitorados;

3.1.22.2. Deverá ser instalado agentes específicos nos servidores e desktops, objetivando coletar informações mais detalhadas para o serviço de monitoramento, desde que seja plenamente compatível com o sistema onde será instalado e não afete o desempenho dos serviços;

3.1.22.3. A análise das informações correlacionadas deve ser realizada com auxílio de bases globais de inteligência cibernética em conjunto com a expertise dos profissionais do fabricante, com vistas a reduzir ao máximo os falsos positivos;

3.1.22.4. É obrigatório que a comunicação entre equipamentos e soluções do fabricante instalados nos dispositivos e qualquer infraestrutura onde esses dados sejam processados ocorra de forma segura, utilizando algoritmos criptográficos para preservar o sigilo das informações;

3.1.22.5. Deverá ser feita a investigação e a classificação dos eventos monitorados, aplicando os principais frameworks de gestão de incidentes de segurança cibernética bem como boas práticas de mercado na detecção e triagem dos eventos de segurança, objetivando minimizar a presença de falsos positivos na abertura de incidentes de segurança;

3.1.22.6. O serviço de monitoramento deverá ser capaz de coletar e realizar a correlação de eventos dos sistemas e ativos monitorados, permitindo uma visão mais abrangente do alcance das ações maliciosas, bem como de possível movimentação lateral do atacante dentro da rede;

3.1.22.7. O monitoramento deverá ser capaz de identificar as principais ameaças, bem como táticas, técnicas e procedimentos de ataque descritos na base de conhecimento MITRE ATT&CK, sem prejuízo do uso de outras bases de conhecimento ou serviços de inteligência de ameaças,para complementação da capacidade de identificação de atividades maliciosas;

3.1.22.8. Deverá monitorar e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média e identificando comportamentos anômalos, visando antecipar a identificação de incidentes de segurança;

3.1.22.9. A solução deverá prover inteligência de proteção contra-ataques cibernéticos a nível global, sendo responsável por pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança monitorados;

3.1.22.10. O fabricante deverá utilizar solução para registro de incidente de segurança, acessível pela equipe técnica da Contratante, para indicar ações de contenção, comunicar à equipe da Contratante sobre o andamento do tratamento dos incidentes

3.1.23. Compatibilidade:

3.1.23.1. É suportada por qualquer um dos seguintes navegadores:

3.1.23.1.1. Apple Safari versões mais recentes;

3.1.23.1.2. Google Chrome versões mais

recentes;3.1.23.1.3. Microsoft Edge;

3.1.23.1.4. Mozilla Firefox versões mais recentes;

3.1.24. Requisitos de rede:

3.1.24.1.1. Em condições médias de carga: um canal full-duplex com largura de banda de pelomenos 1,7 Kbps para cada ativo;

3.1.24.1.2. Em condições de carga máxima: um canal full-duplex com largura de banda de pelomenos 2,7 Kbps para cada ativo;

3.1.25. Compatibilidade de sensor de endpoint

3.1.25.1. O agente de endpoint deve ser compatível com os seguintes sistemas operacionais, para no mínimo a coleta e envio dos dados/telemetria ao SOC do fabricante:

3.1.25.1.1. Microsoft Windows 7 e superiores;

3.1.25.1.2. macOS 10.14-11;

3.1.25.1.3. CentOS 6.7 ou superior;

3.1.25.1.4. Debian GNU / Linux 9.4 ou

superior;3.1.25.1.5. Linux Mint 19 ou

superior;

3.1.25.1.6. Oracle Linux 7.3 ou superior;

3.1.25.1.7. Red Hat Enterprise Linux 6.7 ou superior;

3.1.25.1.8. SUSE Linux Enterprise Server 12 SP5 ou

superior;3.1.25.1.9. Ubuntu 18.04 LTS ou superior.

3.1.26. Capacidades técnicas

3.1.26.1. Deve possuir console web própria do serviço, além de integração nativa com a console do“software de segurança e antivírus para servidores físicos, microcomputadores e smartphones

/tablets”

3.1.26.2. A console deve possuir dashboards com as informações principais, apresentando no mínimo:

3.1.26.2.1. Número de incidentes e status

3.1.26.2.2. Quantidade de dispositivos

monitorados

3.1.26.2.3. Deve possuir mecanismo de notificações, com no mínimo as seguintes opções:

3.1.26.2.4. E-mail

3.1.26.2.5. Telegram

3.1.26.3. Deve permitir o envio de relatórios;

3.1.26.4. O agente deve enviar a telemetria em tempo real para o SoC do fabricante;

3.1.26.5. O serviço deve compreender monitoramento dos dados enviados e alertas gerados emum regime 24x7x265;

3.1.26.6. O envio e armazenamento da telemetria, devem respeitar as principais legislações deproteção de dados, como GDPR e LGPD;

3.1.26.7. O SoC do fabricante deve possuir datacenters em pelo menos duas localidades em diferentes países;

3.1.26.8. O SoC do fabricante deve possuir equipes de analistas em pelo menos 3 regiões (países)incluindo Brasil;

3.1.26.9. Os dados coletados devem passar por no mínimo:

3.1.26.9.1. Modelos de Machine Learning/Inteligência

Artificial;3.1.26.9.2. Análise humana;

3.1.26.9.3. Correlação com IoA's (indicadores de

ataque);3.1.26.9.4. Emulação em sandbox (quando

necessário);

3.1.26.10. Após análise, informações sobre atividades potencialmente maliciosas, devem ser apresentadas no portal como "Incidentes";

3.1.26.11. O Incidente deve possuir no mínimo as seguintes

informações:3.1.26.11.1. Resumo;

3.1.26.11.2. Prioridade (Baixa, Média e Alta);

3.1.26.11.3. Recomendação;

3.1.26.11.4. Data de criação e data de atualização;

3.1.26.11.5. Correlacionamento com táticas/técnicas do Framework MITRE

ATT&CK;3.1.26.11.6. Dispositivos afetados;

3.1.26.11.7. IOCs de host e de rede;

3.1.26.11.8. Descrição completa em linha do tempo;

3.1.26.12. O incidente pode receber ações de resposta recomendada disparadas pela equipe deSoC, compreendendo no mínimo as seguintes ações:

3.1.26.12.1. Transferir arquivo para o

SoC;3.1.26.12.2. Isolar um dispositivo;

3.1.26.12.3. Desabilitar isolamento de

dispositivo;3.1.26.12.4. Deletar chave de

registro; 3.1.26.12.5. Dump de memória;

3.1.26.13. As ações devem ser aprovadas no portal por profissional da contratante, com a opção dehabilitar aprovação automática.

3.1.27. Agente de endpoint

3.1.27.1. As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem seroperadas na mesma console de gerenciamento da solução de endpoint;

3.1.27.2. A solução deve oferecer módulo focado em capacidades de EDR “Endpoint Detection andResponse”, incluindo no mínimo as seguintes capacidades:

3.1.27.3. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e aocontexto da ameaça;

3.1.27.4. Deve fornecer graficamente a visualização da cadeia do ataque;

3.1.27.5. Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).

3.1.27.6. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

3.1.27.6.1. Isolar o host;

3.1.27.6.2. Iniciar uma varredura nas áreas

críticas;3.1.27.6.3. Quarentenar o objeto;

3.1.27.7. A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluirno mínimo os seguintes dados:

3.1.27.7.1. Detecções provenientes da solução de

endpoint;3.1.27.7.2. Processos;

3.1.27.7.3. Alterações de

registro;3.1.27.7.4. Conexões

remotas; 3.1.27.7.5. Criação de

arquivos;

3.1.27.8. Varredura por todos os dispositivos executada a partir de indicador de comprometimento(IoC) gerado através da solução e importado pelo administrador.

3.1.27.9. Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução.

3.1.27.10. A solução deve oferecer no mínimo as seguintes opções de resposta: 3.1.27.10.1. Prevenir a execução de um arquivo;

3.1.27.10.2. Quarentenar um arquivo;

3.1.27.10.3. Iniciar uma varredura por

IoC;3.1.27.10.4. Parar um processo;

3.1.27.10.5. Executar um processo;

3.1.27.11. Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

3.1.27.11.1. A opção de isolamento deve estar disponível junto a visualização do incidente;

3.1.27.11.2. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

ITEM 06 – SOFTWARE DE SEGURANÇA PARA STORAGE

3.1.28. Requerimentos Gerais

3.1.28.1. A solução deve possuir proteção AntiMalware em tempo real;

3.1.28.2. A solução deve ter a capacidade de proteger servidores de arquivos e servidores dearmazenamentos conectados à rede (NAS);

3.1.28.3. Deve possuir gerenciamento, monitoramento e atualizações centralizados;

3.1.28.4. Deve ter a capacidade de conter padrões de ataques baseados em redes;

3.1.28.5. Deve nativamente possuir proteção contra criptografia de pastas e arquivos compartilhados;

3.1.28.6. Deve possuir suporte ao agente CAVA e aos protocolos RCP e ICAP;

3.1.28.7. Deve ser tolerante à falhas e ser escalável;

3.1.28.8. Deve suportar servidores em Cluster;

3.1.28.9. Deve possuir mecanismo de atualização do banco de dados de reputação de malwares, devendo ser do próprio fabricante da solução, com possibilidade de escolha da frequência.

3.1.28.10. Permitir a busca por vários métodos de atualização, incluindo canais de comunicaçãoglobal e recursos compartilhados na rede local.

3.1.28.11. Permitir a verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

3.1.28.12. A console de gerenciamento do computador deve funcionar nas seguintes plataformas Windows

3.1.28.12.1. Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou superior (32/64 bits);

3.1.28.12.2. Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou superior (32/64 bits);

3.1.28.12.3. Windows Server 2008 Standard / Enterprise / Datacenter SP2 ou superior (32/64

bits);3.1.28.12.4. Windows Server 2008 Core ou superior (64 bits);

3.1.28.12.5. Microsoft Small Business Server 2008 Standard / Premium SP2 ou superior (64 bits);

3.1.28.12.6. Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 ousuperior (64 bits);

3.1.28.12.7. Windows Hyper-V Server 2008 R2 SP1 ou superior (64 bits);

3.1.28.12.8. Microsoft Small Business Server 2011 Essentials / Standard SP1 ou superior (64 bits);

3.1.28.12.9. Microsoft Windows MultiPoint Server 2011 Standard / Premium Microsoft Small Business Server 2008 Standard / Premium SP2 ou superior (64 bits);

3.1.28.12.10. Windows Server 2012 Foundation / Essentials / Standard / Datacenter (64

bits);3.1.28.12.11. Microsoft Windows MultiPoint Server 2012 Standard / Premium (64

bits);

3.1.28.12.12. Windows Storage Server 2012 Foundation / Essentials / Standard / Datacenter (64bits);

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

(64bits);3.1.28.12.14. Windows Storage Server 2012 R2 (64bits);

3.1.28.12.15. Windows Hyper-V Server 2012, Windows Hyper-V Server 2012 R2

(64bits);3.1.28.12.16. Windows Server 2016 Essentials / Standard / Datacenter

(64bits); 3.1.28.12.17. Microsoft Windows MultiPoint Server 2016 (64bits);

3.1.28.12.18. Windows Storage Server 2016 Essentials / Standard / Datacenter

(64bits);3.1.28.12.19. Windows Server 2019 Essentials / Standard / Datacenter

(64bits); 3.1.28.12.20. Windows Storage Server 2019 (64bits);

3.1.28.12.21. Microsoft Windows XP Professional SP2 ou superior (32/64

bits);3.1.28.12.22. Microsoft Windows Vista (32/64 bits);

3.1.28.12.23. Microsoft Windows 7 (32/64 bits);

3.1.28.12.24. Microsoft Windows 8 ou superior (32/64

bits);3.1.28.12.25. Microsoft Windows 10 (32/64 bits);

3.1.28.12.26. Windows 10 Redstone 1 à 6 (32/64 bits);

3.1.29. Características para Proteção de Servidores de Arquivos

3.1.29.1. Deve possuir Compatibilidade de instalação com os seguintes sistemas

operacionais: 3.1.29.1.1. Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou superior (32/64bits);3.1.29.1.2. Windows Server 2003 R2 Foundation SP2 ou superior (32bits);

3.1.29.1.3. Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou superior (32/64bits);

3.1.29.1.4. Windows Server 2008 Standard / Enterprise / Datacenter SP2 ou superior(32/64bits);

3.1.29.1.5. Windows Server 2008 Core Standard / Enterprise / Datacenter SP2 ou superior (32 /64bits);

3.1.29.1.6. Microsoft Small Business Server 2008 Standard / Premium SP2 ou posterior (64 bits);

3.1.29.1.7. Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 ou posterior (64 bits);

3.1.29.1.8. Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 ou posterior (64bits);

3.1.29.1.9. Windows Hyper-V Server 2008 R2 SP1 ou posterior (64 bits);

3.1.29.1.10. Microsoft Small Business Server 2011 Essentials / Standard SP1 ou posterior (64 bits);3.1.29.1.11. Microsoft Windows MultiPoint Server 2011 Standard / Premium (64 bits);

3.1.29.1.12. Windows Server 2012 Foundation / Essentials / Standard / Datacenter (64 bits);

3.1.29.1.13. Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter (64 bits);3.1.29.1.14. Microsoft Windows MultiPoint Server 2012 Standard / Premium (64 bits);

3.1.29.1.15. Windows Storage Server 2012 (64 bits);

3.1.29.1.16. Windows Hyper-V Server 2012 (64 bits);

3.1.29.1.17. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (64 bits);

3.1.29.1.18. Windows Server 2012 R2 Core / Foundation / Essentials / Standard / Datacenter (64 bits);

3.1.29.1.19. Windows Storage Server 2012 R2 (64 bits);

3.1.29.1.20. Windows Hyper-V Server 2012 R2 (64 bits);

3.1.29.1.21. Windows Server 2016 Essentials / Standard / Datacenter (64

bits);3.1.29.1.22. Windows Server 2016 MultiPoint (64 bits);

3.1.29.1.23. Windows Server 2016 Core Standard / Datacenter (64

bits);3.1.29.1.24. Microsoft Windows MultiPoint Server 2016 (64

bits);

3.1.29.1.25. Windows Storage Server 2016 (64 bits);

3.1.29.1.26. Windows Hyper-V Server 2016 (64 bits);

3.1.29.1.27. Windows Server 2019 Essentials / Standard / Datacenter (64

bits);3.1.29.1.28. Windows Server 2019 Core (64 bits);

3.1.29.1.29. Windows Storage Server 2019 (64 bits);

3.1.29.1.30. Windows Hyper-V Server 2019 (64 bits);

3.1.29.1.31. Windows 10 Enterprise multi-session (64 bits);

3.1.29.2. A solução de segurança deve fornecer proteção aos servidores de arquivos usando osseguintes servidores de terminal:

3.1.29.2.1. Windows 2008 SP2 Server Microsoft Remote Desktop Services ou

superior;3.1.29.2.2. Windows 2008 R2 Server Microsoft Remote Desktop Services ou superior; 3.1.29.2.3. Windows 2012 Server Microsoft Remote Desktop Services ou superior; 3.1.29.2.4. Windows 2012 Server R2 Remote Desktop Services ou superior; 3.1.29.2.5. Windows 2016 Server Microsoft Remote Desktop Services ou superior; 3.1.29.2.6. Windows 2019 Server Microsoft Remote Desktop Services ou superior; 3.1.29.2.7. Citrix XenApp 6.0, 6.5, 7.0, 7.5 — 7.9, 7.15

3.1.29.2.8. Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15

3.1.29.3. Deve realizar a proteção contra malwares em tempo real e permitir a configuração deverificação agendada;

3.1.29.4. Deve possuir proteção especial contra malware de criptografia de arquivos para recursosde rede compartilhados, fornecendo defesas confiáveis contra Ransomware;

3.1.29.5. Deve possibilitar a proteção baseada em nuvem contra novas ameaças, permitindo que o aplicativo entre em contato com os recursos especializados do fabricante para obter um veredicto de arquivo durante a verificação em tempo real ou programada;

3.1.29.6. Deve permitir a verificação manual ou sob demanda de servidores de arquivos selecionados;

3.1.29.7. Deve permitir o escaneamento de arquivos, pastas ou de todo o sistema selecionado;

3.1.29.8. Deve impedir o re-escanemento de arquivos;

3.1.29.9. Quando atuando no veredicto de um malware, deve no mínimo tomar as seguintes ações:3.1.29.9.1. Bloquear;

3.1.29.9.2. Neutralização;

3.1.29.9.3. Remoção e,

3.1.29.9.4. Notificar os administradores.

3.1.29.10. Deve possuir uma console de gerenciamento única para todos os componentes de proteção;

3.1.29.11. Deve ter a capacidade de excluir arquivos, no mínimo, com as seguintes

bases:3.1.29.11.1. Um nome específico,

3.1.29.11.2. Arquivos localizados em um endereço específico

e,3.1.29.11.3. Arquivos com uma máscara específica.

3.1.29.12. Ter a capacidade importar ou exportar a lista de exclusões de verificação e proteção emtarefas de verificação e perfis de proteção;

3.1.29.13. Ter a capacidade de exportar e importar lista de exceções;

3.1.29.14. Ter a capacidade de criar lista de exceções frequentes compiladas de acordo com asrecomendações da Microsoft;

3.1.29.15. Deve poder realizar o armazenamento de cópias de backup de arquivos excluídos;

3.1.29.16. Dar suporte para o esquema de licenciamento de acordo com a quantidade de servidoresde segurança;

3.1.29.17. Ter suporte para ativação usando um código de ativação fornecido via assinatura;

3.1.29.18. Deve fornecer informações sobre o número de objetos escaneados;

3.1.29.19. Deve fornecer informações sobre detalhes do banco de dados de antivírus;

3.1.30. Características para Proteção de Servidores de Armazenamento conectados à rede (NAS)

3.1.30.1. A solução de suportar a integração com os seguintes servidores

NAS:3.1.30.1.1. NetApp® com um dos seguintes sistemas:

3.1.30.1.1.1. Data ONTAP 7.x and Data ONTAP 8.x 7-mode;

3.1.30.1.1.2. Data ONTAP 8.2.1 Cluster-mode;

3.1.30.1.1.3. Data ONTAP 9.0 – 9.7 Cluster-mode;

3.1.30.1.2. Dell EMC™ Celerra / VNX com os softwares a

seguir:3.1.30.1.2.1. EMC DART 6.0.36 ou mais recente;

3.1.30.1.2.2. Celerra Anti Virus Agent (CAVA) 4.5.2.3 ou mais

recente;3.1.30.1.3. Dell EMC Isilon with OneFS 7.0 ou mais

recente; 3.1.30.1.4. Hitachi NAS (ICAP, RPC):

3.1.30.1.4.1. 12.0 ou mais recente para integração com

ICAP;3.1.30.1.4.2. 11.2 ou mais recente para integração

com RPC; 3.1.30.1.5. IBM System Storage N series;

3.1.30.1.6. Oracle ZFS Storage Appliance;

3.1.30.1.7. Dell NAS na plataforma Dell Compellent™ FS8600:

3.1.30.1.7.1. FluidFS 6.x; 3.1.30.1.7.2. FluidFS 5.x;

3.1.30.1.8. HPE 3PAR com File Persona

3.3.1: 3.1.30.1.8.1. HPE 3PAR StoreServ File Controller;

3.1.30.1.8.2. HPE 3PAR StoreServ 7000c, 8000, 9000, 20000 Storage;

3.1.30.1.9. Nutanix File Storage: 3

.1.30.1.9.1. Nutanix Files 3.8 ou posterior;

3.1.30.2. Deve realizar a proteção contra malwares em tempo real e permitir a configuração de verificação agendada;

3.1.30.3. Deve possibilitar a proteção baseada em nuvem contra novas ameaças, permitindo que o aplicativo entre em contato com os recursos especializados do fabricante para obter um veredicto de arquivo durante a verificação em tempo real ou programada;

3.1.30.4. Deve permitir a verificação manual ou sob demanda de servidores de arquivos selecionados;

3.1.30.5. Deve permitir o escaneamento de arquivos, pastas ou de todo o sistema selecionado;

3.1.30.6. Deve impedir o re-escanemento de arquivos;

3.1.30.7. Quando atuando no veredicto de um malware, deve no mínimo tomar as seguintes

ações:3.1.30.7.1. Bloquear;

3.1.30.7.2. Neutralização;

3.1.30.7.3. Remoção e,

3.1.30.7.4. Notificar os administradores.

3.1.30.8. Deve possuir uma console de gerenciamento única para todos os componentes de proteção;

3.1.30.9. Deve ter a capacidade de excluir arquivos, no mínimo, com as seguintes

bases:3.1.30.9.1. Um nome específico,

3.1.30.9.2. Arquivos localizados em um endereço específico e,

3.1.30.9.3. Arquivos com uma máscara específica.

3.1.30.10. Ter a capacidade importar ou exportar a lista de exclusões de verificação e proteção emtarefas de verificação e perfis de proteção;

3.1.30.11. Ter a capacidade de exportar e importar lista de exceções;

3.1.30.12. Ter a capacidade de criar lista de exceções frequentes compiladas de acordo com asrecomendações da Microsoft;

3.1.30.13. Deve poder realizar o armazenamento de cópias de backup de arquivos excluídos;

3.1.30.14. Dar suporte para o esquema de licenciamento de acordo com a quantidade de servidoresde segurança;

3.1.30.15. Ter suporte para ativação usando um código de ativação fornecido via assinatura;

3.1.30.16. Deve fornecer informações sobre o número de objetos escaneados;

3.1.30.17. Deve fornecer informações sobre detalhes do banco de dados de antivírus;

ITEM 07 – SOFTWARE DE DETECÇÃO CONTRA-ATAQUES COMPLEXOS E DIRECIONADOS

3.1.31. Das capacidades da console de gerenciamento

3.1.31.1. A Console de gerenciamento deve apresentar uma dashboard customizável;

3.1.31.2. Deve apresentar a saúde do sistema, informando quais componentes estão atualizados ounão;

3.1.31.3. Deve mostrar em tempo real o tráfego sendo processado pelos sensores;

3.1.31.4. Deve apresentar em tempo real gráfico de pacotes descartados caso não suporte o tráfego gerado;

3.1.31.5. Deve permitir criar perfis de layout;

3.1.31.6. Deve permitir exportar para PDF o layout atual da solução;

3.1.31.7. Deve mostrar pelo menos as seguintes informações atualizadas sobre a ferramenta:3.1.31.7.1. Saúde do sistema;

3.1.31.7.2. Tráfego em tempo real;

3.1.31.7.3. Top 10 domínios mais acessados;3.1.31.7.4. Mostrar alertas por importância; 3.1.31.7.5. Top 10 Ips mais acessados;

3.1.31.7.6. Alertas por tecnologias de detecção;3.1.31.7.7. Alertas por vetor de ataques;

3.1.31.8. Deve permitir criar novos usuários para acesso à console com pelo menos 3 níveis deacesso;

3.1.31.9. Deve permitir integração com a Console de gerenciamento da ferramenta de antivíruscaso seja necessário a implementação de EDR;

3.1.31.10. Os alertas deverão ser exibidos permitindo visualizar quantos são novos, quantos estãoem processo e quantos já foram processados;

3.1.31.11. Deve mostrar quantidades de eventos pela criticidade, alto, médio ou baixo;

3.1.31.12. Deve permitir exportar os alertas para o formato (.txt);

3.1.31.13. Possibilidade de assinalar um evento para determinado usuário para verificação;

3.1.31.14. Deve suportar arquivos no formato CEF para integração com SIEM;

3.1.31.15. O usuário com conta administrativa deve ter permissão para assinalar um incidente parausuários específicos;

3.1.31.16. Possibilidade de marcar evento como processado para informar que o incidente já foianalisado e resolvido;

3.1.31.17. Deve se possível gerenciar o status de cada evento;

3.1.31.18. As seguintes informações devem ser mostradas nos alertas de

eventos:3.1.31.18.1. Host onde ocorreu o incidente;

3.1.31.18.2. Origem do

ataque;3.1.31.18.3. Destino

do ataque;

3.1.31.18.4. Dia e horário de quanto ocorreu o

ataque;3.1.31.18.5. Nome do objeto considerado

malicioso; 3.1.31.18.6. Tamanho do objeto;

3.1.31.18.7. Hash do objeto em pelo menos MD5 e SHA256;

3.1.31.18.8. URL do ataque;

3.1.31.18.9. Nome da tecnologia responsável por identificar o ataque;

3.1.31.18.10. Informar se o ataque possui características baseado no YARA (Ferramenta

opensource);

3.1.31.18.11. A console de gerenciamento deverá permitir que o administrador procure por eventossimilares na rede baseado no tipo de arquivo, no hash do arquivo, tipo de evento e nome do arquivo;

3.1.31.18.12. Deve permitir a instalação do sensor de endpoint de forma remota;

3.1.31.18.13. Possibilidade de mostrar a sequência de atividades executadas pelo malware quandoexecutada no SandBox;

3.1.31.18.14. Deve permitir fazer uma busca no sistema por eventos baseados em regras;

3.1.31.18.15. Deve permitir fazer buscas de IoCs no banco de dados através de informações recebidas pelos agentes;

3.1.31.18.16. Deve permitir buscar no sistema eventos baseados nas seguintes

categorias:3.1.31.18.16.1. Texto completo;

3.1.31.18.16.2. Por host;

3.1.31.18.16.3. Por tipo de vento;

3.1.31.18.16.4. Por arquivos;

3.1.31.18.16.5. Pelo hash MD5 e

SHA256;

3.1.31.18.16.6. Pela conexão de rede;

3.1.31.18.16.7. Chave de registro;

3.1.31.18.16.8. Eventos do Windows;

3.1.31.18.16.9. Alteração de nome do host;

3.1.31.18.17. Deve permitir importar IOCs (Índices de comprometimento) visando encontrar ataquesde acordo com informações contidas no IoC;

3.1.31.18.18. Capacidade de executar as seguintes tarefas remotamente nos Endpoints que possuem o EDR (Endpoint Detection Response) instalado:

3.1.31.18.18.1. Finalizar processo;

3.1.31.18.18.2. Executar programa;

3.1.31.18.18.3. Coletar arquivo;

3.1.31.18.18.4. Deletar arquivo;

3.1.31.18.18.5. Quarentenar arquivo;

3.1.31.18.18.6. Restaurar arquivo da

quarentena;

3.1.31.18.19. Deve permitir ao coletar um arquivo remotamente enviar automaticamente para oSANDBOX para análise;

3.1.31.18.20. Deve possuir funcionalidade que permita prevenir um arquivo de ser executado em qualquer host com o EDR instalado através do hash MD5/SHA256;

3.1.31.18.21. Deverá possuir capacidade de disponibilizar facilmente as amostras dos arquivossuspeitos detectados e do arquivo PCAP do contexto de captura;

3.1.31.18.22. Deverá permitir o uso de base de conhecimento na Internet do próprio fabricante, com atualização automática de regras e assinaturas, para consultas automáticas em bases de reputação e correlacionamento de informações sobre ameaças conhecidas, identificando assim as respectivas recomendações de ações;

3.1.31.18.23. Deve possuir plataforma de inteligência de ameaças, informando se o ataque fazparte de uma campanha global, quais as regiões e plataformas afetadas pelo ataque, bem como disponibilizar links de referência sobre a ameaça;

3.1.31.18.24. Deve possuir plataforma do próprio fabricante com informações sobre as ameaças, informando título, data descoberta e descrição sobra a ameaça.

3.1.31.18.25. Deve possuir integração com portal de inteligência para avançar na pesquisa a partir dos eventos;

3.1.31.18.26. Deve ser possível realizar consultas de IP, HASH domínios no portal de inteligência do próprio fabricante;

3.1.31.18.27. Para cada malware, Exploits ou componente malicioso, a ferramenta deve possuirlinks para detalhar informações sobre estes;

3.1.31.18.28. Possibilidade de selecionar quais dispositivos serão afetados pela tarefa de prevenção de execução de arquivos;

3.1.31.18.29. Capacidade de baixar arquivos quarentenados diretamente pela console de administração do Anti-APT;

3.1.31.18.30. Capacidade de visualizar quantos Endpoints possuem o EDR instalado através de integração com a Console de gerenciamento do antivírus;

3.1.31.18.31. Deve mostrar quantos Endpoints estão sendo gerenciados informando também quantos não possuem EDR instalado;

3.1.31.18.32. Possuir relatórios customizáveis possibilitando adicionar ou remover colunas de identificação e status de ventos;

3.1.31.18.33. Deve permitir criar relatórios baseados na tecnologia de proteção utilizada;

3.1.31.18.34. Criar relatórios de eventos organizados pelas seguintes severidades: baixa, média ealta;

3.1.31.18.35. Deve permitir adicionar imagens ao relatório;

3.1.31.18.36. Permitir criar listas brancas baseadas nos seguintes

filtros:3.1.31.18.36.1. Por hash MD5;

3.1.31.18.36.2. Por formato;

3.1.31.18.36.3. Por URL;

3.1.31.18.36.4. Por e-mail;

3.1.31.18.36.5. Por Sub-rede;

3.1.31.18.37. Permitir criar regras de notificações para envio por e-mail quando novos eventos sãoidentificados pela ferramenta;

3.1.31.18.38. Deve permitir configurar o status do endpoint de acordo com a quantidade de dias deinatividade;

3.1.31.18.39. Deve permitir integrar a solução com pelo menos as seguintes ferramentas de SIEM:ArchSight, Splunk e IBM Qradar;

3.1.32. Características para o SandBox

3.1.32.1. As Sandboxes deverão suportar os seguintes sistemas

operacionais:3.1.32.1.1. Windows XP x86 Sp3;

3.1.32.1.2. Windows 7 X64;

3.1.32.1.3. Windows 10 x64;

3.1.32.2. Suportar atualização da base de dados da Rede de Inteligência de forma automática esem causar nenhum tipo de indisponibilidade da solução;

3.1.32.3. A análise inicial deve ser realizada de forma local no ambiente de detecção, o envio de artefatos para verificação na SandBox deve ocorrer de forma automática, ou seja, caso a inteligência do produto identifique a necessidade de encaminhar o objeto para análise na SandBox este processo deve ocorrer sem a intervenção de qualquer usuário;

3.1.32.4. A solução deve ser capaz de prover dados forense detalhados, via interface gráfica, relacionados à infecção, demonstrando o ciclo de vida completo do ataque. Estes dados forenses devem incluir a cronologia completa do ataque e não apenas uma porção do ataque, assim como:

3.1.32.4.1. URLs/sites web relacionados ao

ataque;3.1.32.4.2. hashes MD5/SHA256;

3.1.32.4.3. binários maliciosos anexados;

3.1.32.5. Detectar e inspecionar, no mínimo, os seguintes tipos de arquivo, considerando as diferentes versões de sistemas operacionais e aplicativos existentes:

3.1.32.5.1. Arquivos executáveis;

3.1.32.5.2. Scripts;

3.1.32.5.3. Arquivos;

3.1.32.5.4. Documentos do office;

3.1.32.5.5. Arquivos de mídia;

3.1.32.5.6. Arquivos de Android

(APK)

3.1.32.6. A solução deverá prover um método de disponibilizar updates das Sandboxes sem requerer um completo update do sistema operacional ou upgrade da solução e sem indisponibilidade de sua detecção;

3.1.32.7. Toda análise básica de malwares, incluindo malwares desconhecidos, deve ser

realizada de forma automatizada através da detecção do Exploits, sem a necessidade de criação de regras específicas ou interação de um operador;

3.1.32.8. Toda a análise do comportamento do malware deve ser registrada em tempo de execução;

3.1.32.9. A solução deve suportar importação de regras YARA personalizadas, para permitir flexibilidade na criação de regras para análise de ameaças;

3.1.32.10. Suportar mecanismo de whitelist pelos seguintes métodos:

3.1.32.10.1. Hash MD5 do

arquivo;3.1.32.10.2. Formato do

arquivo; 3.1.32.10.3. E-mail;

3.1.32.10.4. Sub-rede.

3.1.32.11. Deve permitir o envio de alertas por e-mail;

3.1.32.12. A solução deverá suportar mais de um SandBox em cluster, permitindo o escalonamento baseado na necessidade do contratante;

3.1.32.13. Deverá possuir a capacidade de detectar ameaças direcionadas, realizando inspeção de tráfego até a camada 7 de forma a prevenir ataques do dia zero e executar análise profunda de documentos que contenham conteúdo malicioso ou redirecionamentos para outras URLs maliciosas;

3.1.32.14. O SandBox da solução deve possuir mecanismos para prevenção de evasão.

3.1.33. Sensores de detecção

3.1.33.1. A solução deverá permitir que o sensor monitore tráfego WEB, Mail e Rede;

3.1.33.2. Deverá permitir integração com solução de proxy utilizando o protocolo ICAP permitindo analisar protocolos seguros (exemplo: HTTPS);

3.1.33.3. Deverá verificar mensagens de e-mail através do protocolo POP3 e SMTP;

3.1.33.4. Deverá processar tráfego espelhado e extrair objetos e metadados do DNS

3.1.33.5. A solução deve suportar um throughput de análise de no máximo 4000 Mbps;

3.1.33.6. A solução deverá ser gerenciada por console Web suportando no mínimo os browsers Internet Explorer e Firefox;

3.1.33.7. Deve permitir configurar mais de um sensor de rede caso o ambiente corporativo tenha mais de um ponto para análise;

3.1.33.8. Deverá possuir a capacidade de atualizar as vacinas do sensor pela internet ou através da console de gerenciamento;

3.1.33.9. O Sensor de rede deverá suportar SPAN Port ou TAP para análise do tráfego;

3.1.33.10. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;

3.1.33.11. O sensor deverá encaminhar automaticamente para a SandBox um artefato potencialmente perigoso identificado no tráfego de rede;

3.1.33.12. O sensor deverá alertar qualquer artefato malicioso identificado já conhecido sem a necessidade de intervenção manual;

3.1.33.13. Deverá detectar incidentes de segurança motivados por conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos além da detecção de malwares conhecidos e desconhecidos, Ransomware, Exploits, Botnets, Cross Site Script, SQL

Injection, comunicações p2p, Instant Messengers; streaming, tentativas de scan de rede, tentativas de brute - force, situações de evasão e roubo de informação etc.;

3.1.33.14. Deverá ter capacidade de verificar em tempo real a reputação de endereços web (URLs)e servidores de correio SMTP;

3.1.33.15. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística;

3.1.33.16. Deverá atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;

3.1.33.17. Deve permitir utilizar um sensor de rede como proxy, ou seja, deve permitir que o sensor receba informações do Endpoint para enviar à console de gerenciamento;

3.1.33.18. O Sensor deverá detectar sites maliciosos através de reputação;

3.1.33.19. O sensor deverá ter acesso a rede global de inteligência da fabricante;

3.1.33.20. Deverá integrar com a infraestrutura extraindo objetos do tráfego de rede e efetuandouma análise inicial;

3.1.33.21. Deverá receber objetos para serem verificados dos switches, servidores de proxy e servidores de email;

3.1.33.22. Deverá atuar como IDS na rede detectando anomalias no tráfego de rede e alertando a console de gerenciamento sobre os eventuais incidentes;

3.1.33.23. Caso necessário, deve suportar uma arquitetura única atuando como sensor de rede e console de gerenciamento em uma mesma máquina virtual;

3.1.33.24. Através de consulta na base global da fabricante, deverá detectar os seguintes

itens:3.1.33.24.1. Endereços envolvidos em campanhas de ataques persistentes;

3.1.33.24.2. Servidores de “Command &

Control”;3.1.33.24.3. Sites maliciosos;

3.1.33.24.4. Sites de phishing;

3.1.33.25. Deverá possuir tecnologia de cache para evitar envio de solicitações duplicadas;

3.1.33.26. Deve possuir capacidade de verificar links ativos em documentos do office;

3.1.33.27. O sensor de endpoint deve ser compatível com fabricantes terceiras, permitindo que colete e envie informações a console de gerenciamento sem causar conflito com a atual solução de antivírus.

ITEM 08 – SOFTWARE DE PREVENÇÃO CONTRA A PERDA DE DADOS

3.1.34. Gerenciamento da solução

3.1.34.1. A solução deve fornecer uma estrutura de política única em todos os canais de exfiltração de dados (por exemplo, e-mail, Web, aplicativos SaaS, Impressão, aplicações, Mídia Removível, Compartilhamento de Arquivos);

3.1.34.2. Todas as funções de gerenciamento, incluindo alterações de configuração e upgrades, devem ser conduzidas a partir de um console central;

3.1.34.3. O sistema deve apoiar o acesso baseado em funções e a administração delegada com funções prédefinidas e personalizáveis:

3.1.34.3.1. Auditor;

3.1.34.3.2. Gerente de

Incidentes;3.1.34.3.3. Gerente

de Políticas; 3.1.34.3.4. Super

Administrador;

3.1.34.3.5. Administrador

3.1.34.4. A solução proposta deve oferecer suporte à integração com Active Directory ou File Directory (CSV);

3.1.34.5. A solução deve oferecer suporte à criação/exceção de política com base no diretório de usuário/grupo, máquina, rede, domínio;

3.1.34.6. A solução deve ter a capacidade de auditar alterações (por exemplo, logon/off, alterações de regras, logs do sistema, logs de tráfego);

3.1.34.7. Capacidade de o sistema notificar quando está tendo problemas de conexão;

3.1.34.8. Capacidade de integração (via syslog ou extração de banco de dados) com ferramentas de SIEM para fins de registro e alerta;

3.1.34.9. A solução deve fornecer escalabilidade futura para todos os componentes integrantes da arquitetura que compõe o sistema de DLP;

3.1.34.10. A solução deve oferecer suporte a ambientes de infraestrutura virtualizados, como Azure ou AWS para o portal de gerenciamento, banco de dados e outros componentes.

3.1.34.11. A solução deve ter integração nativa com Classificações de Dados (Boldon James, Microsoft AIP, Seclore, Titus).

3.1.34.12. A solução proposta deve ser capaz de implantar o agente usando métodos comuns de implantação de software, como GPO, SCCM, JAMF etc.

3.1.34.13. A solução deve fornecer a capacidade de verificar o status do agente e relatar

quaisqueragentes que não estejam funcionando corretamente;

3.1.34.14. As comunicações com os módulos da solução e sistemas integrados devem ser criptografadas, via https (entrada/saída);

3.1.34.15. A solução deve oferecer suporte ao Microsoft RMS;

3.1.34.16. A solução deve usar um banco de dados relacional corporativo, como SQL;

3.1.34.17. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade parainstalação, no mínimo, nos sistemas operacionais:

3.1.34.17.1. Windows Server 2008 R2 SP1;

3.1.34.17.2. Windows Server 2012;

3.1.34.17.3. Windows Server 2012 R2;

3.1.34.17.4. Windows Server 2016;

3.1.34.18. Liste os sistemas operacionais e o suporte de versão para Endpoints, VDI, Browsers etc.

3.1.34.19. A arquitetura da solução deve oferecer suporte a sites remotos e usuários de rede distribuídos em muitos locais diferentes.

3.1.34.20. A solução deve descrever em meios de implantação típicos e onde cada componentereside;

3.1.34.21. A solução deve oferecer suporte à autenticação de dois fatores para acesso do administrador ao console de gerenciamento;

3.1.34.22. A solução deve ter uma API RESTful disponível para incidentes de obtenção e atualização;

3.1.34.23. Solução deve ser capaz de ser implantada em Máquinas Virtuais AWS EC2 e Azure;

3.1.34.24. Configuração de políticas de segurança de dados e detecção de conteúdo confidencial;

3.1.34.24.1. A solução deve ter políticas específicas de conformidade "prontas para uso" com base na região e no tipo de setor;

3.1.34.24.2. A solução deve ter políticas pré-definidas (1500+) baseadas em RegEX, Dicionários ou Scripts e deve ser capaz de selecionar políticas com base na correlação do país e das indústrias;

3.1.34.24.3. A solução deve fornecer políticas predefinidas para identificar possíveis expressões que sejam indicativas de cyberbullying, padrões autodestrutivos ou descontentamento dos funcionários;

3.1.34.24.4. A solução deve ter políticas de Indicadores de Risco de Roubo de Dados (por exemplo, e-mail para concorrentes, currículos etc.);

3.1.34.24.5. A solução deve ter a capacidade de usar uma única política para varrer os dados onde quer que sejam armazenados, transmitidos ou usados, tanto na rede quanto no terminal;

3.1.34.24.6. A solução deve permitir modificar os canais de destino podem para quaisquer políticas. (Exemplo: incluir em uma política utilizando o protocolo SMTP, poder incluir os protocolos HTTP e HTTPS;

3.1.34.24.7. Deve configurar exceções baseadas em regras de forma simples evitando geração de falsos positivos;

3.1.34.24.8. A solução deve permitir uma sintaxe flexível para vincular dados a aplicativos específicos, servidores de arquivos, compartilhamentos de rede, impressoras e padrões de

conteúdo exclusivos;

3.1.34.24.9. A solução deve oferecer suporte a tipos de arquivo verdadeiros predefinidos;

3.1.34.24.10. A solução deve oferecer suporte a condições de políticas com base na lógica booleana (AND, OR, NOT);

3.1.34.24.11. A solução deve suportar dados confidenciais em diferentes idiomas, incluindo, mas não limitando o suporte para português do Brasil e Inglês;

3.1.34.24.12. A solução deve extrair e inspecionar o conteúdo baseado em texto de arquivos e anexos;

3.1.34.24.13. A solução deve analisar os metadados do arquivo;

3.1.34.24.14. A solução deve oferecer suporte a impressão digital de arquivo parcial e de hash completo para todos os canais de exfiltração de dados;

3.1.34.24.15. A solução deve distinguir entre diferentes tipos de PII ou PHI. Exemplo: Distinguir entre os nove dígitos sociais de um cliente (CPF) e número de segurança de um número de telefone de nove dígitos sem a presença de uma palavra-chave;

3.1.34.24.16. A solução deve suportar a inspeção de tipos de arquivos de arquivos (ZIP, TAR) para detectar o conteúdo com impressão digital;

3.1.34.24.17. A solução deve suportar a análise de arquivos e anexos grandes (20 MB e maiores) durante o processo de impressão digital do conteúdo;

3.1.34.24.18. A solução deve fornecer um método para dados de impressão digital, como registros de clientes (dados estruturados);

3.1.34.24.19. A solução deve proteger pelo menos 10 milhões de linhas de conteúdo específico

de um banco de dados de informações confidenciais sem depender de palavras-chave ou padrões;

3.1.34.24.20. A solução deve oferecer suporte a um método de detecção de aprendizado de máquina para códigos-fonte, formulários;

3.1.34.24.21. A solução deve suportar regras totalmente personalizáveis com expressões regulares, palavraschave, frases-chave e dicionários;

3.1.34.24.22. A solução deve oferecer suporte ao conteúdo da lista de permissões para removercom segurança a detecção de conteúdo textual;

3.1.34.24.23. A solução deve oferecer suporte à detecção de várias palavras-chave com base emum peso especificado;

3.1.34.24.24. A solução deve suportar pelo menos 5.000 listas de palavras-chave exclusivas;

3.1.34.24.25. A solução deve suportar correspondência de padrões combinada com validação. Por exemplo, detectar padrões comuns de números de cartão de crédito como bem como fazer avalidação da soma de verificação para garantir um número de cartão de crédito válido;

3.1.34.24.26. A solução deve detectar formatos de arquivo criptografados conhecidos e desconhecidos;

3.1.34.24.27. A solução deve identificar tags de classificação de terceiros, Proteção de Informações do Azure ou outras soluções de classificação de dados;

3.1.34.25. Configuração de proteção para estações de trabalho:

3.1.34.25.1. O agente da solução deve ser compatível com MacOS e Windows OS;

3.1.34.25.2. O agente da solução deve ser compatível com Vmware Horizon e Citrix

XenApp;

3.1.34.25.3. O agente da solução deve fornecer proteção contínua de dados confidenciais, independentemente de o usuário estar dentro ou fora da rede. A última política aplicada deverá

ser sempre a política padrão;

3.1.34.25.4. A solução deve detectar tentativas do usuário de enviar dados confidenciais por e-maile Web (HTTP/S);

3.1.34.25.5. A solução deve impedir que os usuários enviem dados confidenciais através de qualquer aplicativo no computador;

3.1.34.25.6. A solução deve impedir a exfiltração de dados por meio de mídia removível (por exemplo, unidades USB);

3.1.34.25.7. A solução deve ser capaz de aplicar políticas diferentes mesmo quando os usuáriosestão usando o mesmo endpoint;

3.1.34.25.8. As tarefas de descoberta de dados de endpoint devem ter uma opção de

agendamento:3.1.34.25.8.1. uma vez;

3.1.34.25.8.2. diariamente;

3.1.34.25.8.3. semanalmente;

3.1.34.25.8.4. continuamente

3.1.34.25.9. A tarefa de descoberta de dados de endpoint deve ter configurações flexíveis para verificar apenas quando o computador estiver ocioso ou pausar a verificação enquanto o computador estiver funcionando com baterias;

3.1.34.25.10. A tarefa de descoberta de dados deve oferecer suporte à inclusão e exclusão por tipo de arquivo, pastas, idade ou tamanho;

3.1.34.25.11. A tarefa de descoberta de dados deve oferecer suporte a opções de varredura completas e diferenciais;

3.1.34.25.12. A descoberta de dados deve ter uma opção para preservar o tempo de acesso original;

3.1.34.25.13. O agente da solução deve aproveitar as tags de rótulos de metadados MIP ou Boldon James para impor a classificação ou reclassificar quando um arquivo violar uma política de dados em repouso

3.1.34.25.14. O agente precisa ser auto-regenerativo e resistente a adulterações;

3.1.34.25.15. Deve monitorar a área de transferência do sistema operacional e tomar medidas com base nos dados copiados e/ou protegidos;

3.1.34.25.16. A solução precisa oferecer suporte a opções de implantação de sistemas operacionais virtualizados;

3.1.34.25.17. O agente precisa oferecer uma mensagem pop-up que possa conter informações customizadas quando o usuário violar uma política;

3.1.34.25.18. A mensagem pop-up deve fornecer uma oportunidade para fornecer justificativa comercial quando a política permitir esta ação;

3.1.34.25.19. A justificativa do usuário deve ser registrada/armazenada em um método que possa ser lido por outros sistemas";

3.1.34.25.20. Os arquivos copiados para dispositivos removíveis devem ser criptografados e o conteúdo deve ser legível apenas em ativos de propriedade da empresa;

3.1.34.25.21. O agente deve oferecer suporte à visibilidade de dados copiados para dispositivos de mídia removível específicos;

3.1.34.25.22. O agente da solução deve oferecer suporte à criptografia de nível de administrador e senha de auto criptografia para o usuário quando os arquivos são copiados para mídia removível;

3.1.34.25.23. O agente de endpoint precisa ter o mínimo ou nenhum impacto no desempenho da máquina.

3.1.34.25.24. O agente da solução deve oferecer suporte a políticas hierárquicas de usuário/grupo com correção/resposta configuráveis;

3.1.34.25.25. O agente da solução deve ser compatível com os navegadores Edge Chromium, Firefox, Safari (Apple) e Chrome;

3.1.34.25.26. O agente da solução deve oferecer suporte ao monitoramento e bloqueio de dados confidenciais carregados para aplicativos em nuvem não autorizados e armazenamento em nuvem;

3.1.34.25.27. O agente da solução deve oferecer suporte a um processo para desabilitar o agentedo endpoint com autorização;

3.1.34.25.28. O agente da solução deve oferecer suporte à capacidade de confiar no aplicativo, configurando- o para não ser monitorado;

3.1.34.25.29. O agente da solução deve oferecer suporte às seguintes operações em dados confidenciais que podem ser executadas nas estações de trabalho:

3.1.34.25.29.1. Copiar e colar controles (ou seja, atividades da área de

transferência); 3.1.34.25.29.2. Controle de impressão em impressoras locais ou de

rede; 3.1.34.25.29.3. Salvar conteúdo em diferentes locais, incluindo salvar em:

3.1.34.25.29.4. Pastas locais; 3.1.34.25.29.5. Compartilhamentos de arquivos

remotos;

3.1.34.25.29.6. Unidades removíveis conectadas a um sistema de endpoint, como unidades

USB;3.1.34.25.29.7. Salvar em locais de armazenamento em nuvem;

3.1.34.26. Configuração de proteção para Dados em Repouso:

3.1.34.26.1. A solução deve oferecer suporte à verificação de dados em repouso no endpoint;

3.1.34.26.2. A solução deve suportar SMB, NFS e CIFS para compartilhamentos de arquivos baseados em Windows e não Windows;

3.1.34.26.3. As tarefas de descoberta de dados devem ter uma opção de agendamento: uma vez, diariamente, semanalmente ou continuamente;

3.1.34.26.4. A tarefa de descoberta de dados deve oferecer suporte à inclusão e exclusão por tipode arquivo, pastas, idade ou tamanho;

3.1.34.26.5. A tarefa de descoberta de dados deve oferecer suporte a opções de varredura diferencial e completa;

3.1.34.26.6. A descoberta de dados deve ter uma opção para preservar o tempo de acesso original;

3.1.34.26.7. A descoberta de dados deve oferecer suporte à alocação de largura de banda para verificação do processo de descoberta;

3.1.34.27. Gerenciamento de incidentes

3.1.34.27.1. A solução deve fornecer a capacidade de escalar incidentes críticos para gerentes ou proprietários de dados;

3.1.34.27.2. A solução deve fornecer controles de segurança e acesso em torno do caso/incidente (usuário e grupo);

3.1.34.27.3. A solução deve atribuir incidentes/casos a usuários de diferentes Unidades de Negócios;

3.1.34.27.4. A solução deve permitir a definição e o estabelecimento de fluxos de trabalho específicos (ou seja, adicionar todos os três tipos de eventos aos casos), atribuir casos a usuários

/proprietári os individuais, permitir que os usuários adicionem notas etc;

3.1.34.27.5. A solução deve oferecer suporte ao monitoramento e gerenciamento de aspectos críticos e fases de cada incidente/caso e fases de cada incidente/caso até a resolução, envolvendo administradores autorizados especificados e usuários específicos da função, conforme necessário durante todo o processo;

3.1.34.27.6. A solução deve fornecer a capacidade de mostrar apenas determinados incidentes de um departamento específico ao ponto focal atribuído desse departamento;

3.1.34.27.7. A solução deve fornecer a capacidade de liberar automaticamente um e-mail em quarentena, postar a aprovação do gerente sem qualquer intervenção manual no console DLP;

3.1.34.27.8. A solução deve oferecer suporte a scripts de correção para planos de ação de DLP(por exemplo, quando um arquivo viola as políticas de DLP, as soluções deixam um arquivo de exclusão com uma notificação);

3.1.34.27.9. A solução deve oferecer suporte ao Fluxo de Incidentes (Workflow) via API para liberar e-mails de quarentena;

3.1.34.28. Relatórios

3.1.34.28.1. A solução deve permitir a investigação de incidentes envolvendo dados em repouso, dados em uso e dados em movimento a partir de um console de gerenciamento centralizado;

3.1.34.28.2. A solução deve fornecer resumo e agrupamento de relatórios personalizados em diferentes variáveis e atributos;

3.1.34.28.3. A solução deve suportar exportações de relatórios de incidentes via planilha, XML, PDFou HTML;

3.1.34.28.4. A solução deve ter relatórios pré-definidos para auxiliar nas investigações;

3.1.34.28.5. A solução deve suportar a capacidade de salvar relatórios personalizados e filtros de incidentes;

3.1.34.28.6. A solução deve suportar a capacidade de definir permissões de relatórios por departamentos;

3.1.34.28.7. A solução deve usar análise de dados avançada para fornecer à sua equipe de operações de segurança um relatório de classificação de pilha sobre os principais riscos de segurança de dados em sua organização;

3.1.34.28.8. A solução deve ser capaz de gerar relatórios programados;

3.1.34.28.9. A solução deve fornecer relatórios flexíveis de incidentes (diário, semanal, mensal, trimestral etc.);

3.1.34.28.10. A solução deve ser capaz de relatar o número de alertas gerados por destino;

3.1.34.28.11. A solução deve permitir que os usuários criem mensagens de alerta personalizáveis para administradores, usuários e gerentes de usuários;

3.1.34.28.12. A solução deve fornecer um catálogo de relatórios abrangente que forneça um "drill-down" para facilitar a investigação dos incidentes de maior risco;

3.1.34.28.13. A solução deve ser capaz de fornecer dados forenses dentro do mesmo registro de incidente.

3.1.34.28.14. A solução deve priorizar instantaneamente casos de níveis de risco alto a baixo com limites de pontuação de risco personalizáveis fornecidos em uma pilha de relatórios de classificação de risco de incidente;

3.1.34.28.15. A solução deve capturar dados de eventos com metadados apropriados (data/hora, usuário, protocolo);

3.1.34.28.16. A solução deve suportar um protocolo de cadeia de custódia;

3.1.34.28.17. A solução deve reter os logs por pelo menos um ano, se não for possível, a solução deve oferecer suporte ao arquivamento de incidentes;

3.1.34.28.18. A solução deve ter a capacidade de alterar a

gravidade:3.1.34.28.18.1. Alta;

3.1.34.28.18.2. Média;

3.1.34.28.18.3. Baixa

3.1.34.28.19. A solução deve ter a capacidade de alterar seu o status:

3.1.34.28.19.1. Novo;

3.1.34.28.19.2. Em Processo;

3.1.34.28.19.3. Fechado;

3.1.34.28.19.4. Falso Positivo;

3.1.34.28.19.5. Escalado.

ITEM 09 - CONTRATAÇÃO DE SOFTWARE DE MONITORAMENTO DE APLICAÇÕES E INFRAESTRUTURA DE REDES E SERVIDORES

3.1.35. Solução de monitoramento de aplicações e infraestrutura de redes e servidores, com tecnologia para mapear todos os dispositivos conectados à rede, criação de Mapas de Topologia, fornecendo uma visibilidade aprofundada tanto em ambientes locais quanto na nuvem.

3.1.36. Deverá fornecer insights detalhados de desempenho e integridade dos sistemas, identificação de gargalos e otimização de desempenho, gerenciamento de configurações, correlacionamento de dados usando técnicas de AIOps, emitir alertas quando ocorrem eventos importantes e criar relatórios personalizados para análise e tomada de decisões, contemplando:

3.1.37. Gerenciamento de redes que permite detectar, diagnosticar e resolver rapidamente problemas de desempenho e falhas de rede, simplificando a detecção, o diagnóstico e a resolução de problemas;

3.1.38. Informações sobre o tempo de resposta, disponibilidade e tempo de atividade de roteadores, switches e outros dispositivos habilitados SNMP;

3.1.39. Apresentação do desempenho em tempo real através de mapas de rede navegáveis e dinâmicos por meio de estatísticas;

3.1.40. Deverá conter Painéis de controle, alertas, relatórios e orientações especializadas prontos para uso sobre os itens gerenciados;

3.1.41. Deverá realizar o descobrimento automático dos dispositivos de rede habilitados para SNMP

/WMI;

3.1.42. Implementação de Solução de caminho de rede (mapa de rede): Deverá executar uma análise e visibilidade profunda dos caminhos críticos de rede desde a origem até o destino mostrando visualmente o tráfego de cada nó (passo a passo);

3.1.43. Apresentação da pilha de desempenho com objetivo de correlacionar os dados e acelerar a identificação da causa raiz, de forma intuitiva através das métricas de desempenho diretamente em um cronograma para correlação visual imediata entre todos os dados;

3.1.44. Captura dos dados de fluxos contínuos de tráfego de rede e apresentar em gráficos de fácil interpretação e tabelas que quantificam exatamente como a rede corporativa está sendo usada e com que finalidade;

3.1.45. Oferecer uma visão ampla e personalizável do seu tráfego de rede em uma só

console

/página;

3.1.46. Analisar dados do NetFlow, J-Flow, sFlow, IPFIX e Huawei NetStream™ nos principais dispositivos de mercado como: Cisco Systems®, Extreme Networks®, HP®, Juniper®, Nortel Networks® e outros grandes fornecedores;

3.1.47. Informações sobre quais aplicativos estão consumindo mais da largura de banda da rede;

3.1.48. Oferecer notificações de alertas instantâneos, seus principais comunicadores, quando uma interface excede seu limite de utilização de largura de banda;

3.1.49. Capacidade de rastrear, gerenciar e planejar o uso de endereços IP e outros recursos relacionados em um ambiente de rede;

3.1.50. Permitir que os administradores executem a administração de serviços de DNS (Sistema de Nomes de Domínio) e Protocolo de Configuração Dinâmica de Host (DHCP), que atribuem e resolvem endereços IP para máquinas;

3.1.51. Fornecimento de funções para agilizar o processo de gerenciamento de endereços IP, coma capacidade de controlar as reservas de endereços IP em DHCP, agregação de dados e relatórios;

3.1.52. Rastreamento e monitoramento dos dados, desde endereços IP atualmente em uso até os dispositivos e usuários associados a esses endereços.

3.1.53. Centralizar o monitoramento de dados em uma única console, o software de gerenciamento de IP deverá fornecer insights críticos sobre elementos de gerenciamento de rede para acelerar a solução de problemas, planejamento de endereços IP e relatórios;

3.1.54. Gerenciamento dos riscos e requisitos de acesso à rede associados ao aumento dos dispositivos IP, oferecendo rastreamento automatizado de usuários e dispositivos, juntamente com recursos avançados de gerenciamento de portas de switch, para controlar, usuários e dispositivos que estão conectados na rede;

3.1.55. A solução deverá ter aos gerenciamentos mínimas listadas abaixo:

3.1.55.1. Gerenciamento de LOGs:

3.1.55.1.1. Deve ser capaz de aceitar Syslog, traps SNMP e eventos do Windows de servidores e dispositivos de rede;

3.1.55.1.2. Deve fornecer console interativo para visualizar dados de

eventos; 3.1.55.1.3. Deve fornecer console interativo para exibir eventos

em tempo real;3.1.55.1.4. Deve fornecer recurso de pesquisa rápida em

eventos;

3.1.55.1.5. Deve permitir a personalização de filtros para restringir os resultados da

pesquisa;3.1.55.1.6. Deve permitir a marcação de eventos com tags codificadas por

cores;

3.1.55.1.7. Deve oferecer suporte a regras personalizadas para descartar mensagens indesejadas;

3.1.55.1.8. Deve oferecer suporte a condições de alerta personalizadas com escopo de fonte dealerta personalizável;

3.1.55.1.9. Deve apoiar a execução de programa externo como ações de

alerta;3.1.55.1.10. Deve ter regras internas para uso imediato e para

personalização;

3.1.55.1.11. Deve suportar o encaminhamento de alerta para a solução de monitoramento NOC ououtros sistemas;

3.1.55.1.12. Deve ter integração do Microsoft Active Directory para contas de usuário;

3.1.55.1.13. Deve fornecer um painel dinâmico que permita visibilidade detalhada e correlacione

o syslog com pontos de dados históricos diferentes em diferentes partes da infraestrutura. O resultado deve ser exportável com um formato tabular;

3.1.55.1.14. A solução de gerenciamento de logs proposta deve se integrar diretamente às soluções de monitoramento e exibir dados de log junto com o desempenho da rede e dos sistemas nomesmo painel;

3.1.55.1.15. A solução de monitorização proposta deve proporcionar a capacidade de armazenamento a longo prazo e de recuperação das mensagens de registo originais;

3.1.55.2. Gerenciamento de Configuração do Servidor:

3.1.55.2.1. A solução de gerenciamento proposta deve ser capaz de fazer backup automático da configuração baseada em texto em sistemas baseados no Windows;

3.1.55.2.2. Deve detectar e exibir alterações para os seguintes itens:

3.1.55.2.2.1. Arquivo de configuração do

aplicativo;3.1.55.2.2.2. Inventário de hardware;

3.1.55.2.2.3. Inventário de software;

3.1.55.2.2.4. Registro do Windows;

3.1.55.2.2.5. Arquivo baseado em

texto;3.1.55.2.2.6. Arquivo binário;

3.1.55.2.3. Deve disparar alerta quando a alteração de configuração acontecer, com a comparaçãode quais linhas de configuração foram adicionadas, excluídas e modificadas;

3.1.55.2.4. Deve permitir que a configuração da linha de base seja usada como ponto de referênciapara comparação de alterações de configuração;

3.1.55.2.5. Deve permitir a comparação da configuração atual com a do passado para entender asmudanças ocorridas ao longo do tempo;

3.1.55.2.6. Deve detectar e exibir alterações no inventário de hardware, incluindo, mas não limitadoa:

3.1.55.2.6.1. Processadores;

3.1.55.2.6.2. Módulos de

memória;3.1.55.2.6.3. Discos

rígidos;

3.1.55.2.6.4. Controladores de

armazenamento;3.1.55.2.6.5. Placa de vídeo;

3.1.55.2.6.6. Interfaces de

rede;3.1.55.2.6.7. Mídia

removível;

3.1.55.2.7. Deve detectar e exibir alterações no inventário de software, incluindo, mas não limitadoa:

3.1.55.2.7.1. Software instalado;

3.1.55.2.7.2. Atualizações do sistema

operacional;3.1.55.2.7.3. Firmware;

3.1.55.2.7.4. Drivers;

3.1.55.2.8. A solução de gerenciamento proposta deve ser capaz de descobrir servidores na rede na entrada de:

3.1.55.2.8.1. Intervalos de endereços

IP;3.1.55.2.8.2. Sub-redes;

3.1.55.2.8.3. Endereços IP individuais;

3.1.55.2.9. Deve ter opção para ativar/desativar a adição automática de nós descobertos;

3.1.55.2.10. Deve fornecer informações de fim de vida/fim de suporte (EoL/EoS) para ajudar amanter os dispositivos atualizados em relação à contratação e manutenção da implantação;

3.1.55.2.11. Deve fornecer um painel dinâmico que permita visibilidade aprofundada e correlatos de pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável com um formato tabular;

3.1.55.2.12. Deve permitir o acesso remoto a recursos e funções relacionados ao trabalho e permitir o acesso remoto para editar e atualizar as configurações do dispositivo;

3.1.55.2.13. Deve permitir que vários usuários façam login ao mesmo tempo;

3.1.55.2.14. Deve fornecer seções separadas para tarefas de gerenciamento de configuração, inventário e relatórios sobre violações de políticas;

3.1.55.2.15. Deve destacar rapidamente dispositivos que não foram copiados para configuração, aqueles com conflitos na configuração etc.;

3.1.55.2.16. Deve se integrar ao Active Directory® para fins de login do usuário;

3.1.55.2.17. A solução de gestão proposta deve fornecer relatórios prontos para uso para várias estatísticas monitoradas;

3.1.55.2.18. Deve permitir a personalização de relatórios adicionando/removendo colunas, definindo filtros, especificando prazos, agrupando colunas etc.;

3.1.55.2.19. Deve permitir que os relatórios sejam enviados dentro do cronograma como relatórios

diários, semanais e mensais;

3.1.55.2.20. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;

3.1.55.2.21. Deve ser capaz de fazer backup da configuração, executar script de configuração e mostrar as últimas alterações de configuração como ações de alerta;

3.1.55.2.22. Deve ter várias ações disponíveis, incluindo, mas não limitado a envio de e-mails, encaminhamento de traps SNMP, execução de executáveis, envio de alertas de texto SMS, reprodução de som, envio de e-mail para uma página da Web, etc.

3.1.55.2.23. A solução de gerenciamento proposta deve permitir o agrupamento de dispositivos por várias propriedades:

3.1.55.2.23.1. por fornecedor;

3.1.55.2.23.2. tipo de máquina; versão do sistema

operacional;3.1.55.2.23.3. outras propriedades

personalizadas;

3.1.55.2.24. Deve ser capaz de integrar com módulos que servem outros fins de monitoramento efornecer uma visão de painel único

3.1.55.2.25. Deve oferecer suporte a várias opções de implantação:

3.1.55.2.25.1. Implantação centralizada;

3.1.55.2.25.2. Implantação distribuída;

3.1.55.2.25.3. Implantação híbrida;

3.1.55.2.26. Com uma exibição centralizada do console de operações, confirmação de

alertas einterface de relatórios; 3.1.55.3. Monitoramento de desempenho:

3.1.55.3.1. A solução de monitoramento proposta deve ser capaz de

monitorar:3.1.55.3.1.1. Roteadores;

3.1.55.3.1.2. Switches;

3.1.55.3.1.3. Firewalls;

3.1.55.3.1.4. Dispositivos sem

fio;3.1.55.3.1.5. Servidores;

3.1.55.3.1.6. Outros dispositivos habilitados para SNMP;

3.1.55.3.2. Deve fornecer automaticamente estatísticas de desempenho de rede aprofundadas e em tempo real após a descoberta/configuração de dispositivos, incluindo, entre outros:

3.1.55.3.2.1. Carga de CPU;

3.1.55.3.2.2. Utilização de

memória; 3.1.55.3.2.3. Utilização

da interface;3.1.55.3.2.4. Perda de

pacotes

3.1.55.3.3. Deve mostrar estatísticas como largura de banda da interface, tráfego atual em bps, total de bytes recebidos/transmitidos etc.;

3.1.55.3.4. Deve ser capaz de descobrir e solucionar problemas de caminhos de rede com detalhes, tanto para ambientes locais quanto na nuvem, de conexões TCP específicas;

3.1.55.3.5. Deve exibir informações que incluem emissão de alertas dos principais protocolos de roteamento (BGP, OSPF, RIP, EIGRP) com opções para exibir e pesquisar tabelas de roteamento, incluindo VRFs, mudanças em rotas padrão e rotas oscilantes, topologia de roteadores e status de vizinhos;

3.1.55.3.6. Deve ajudar com o monitoramento de informações de tráfego multicast e emissão de alertas que incluem informações de topologia, informações multicast, informações de rotas, erros de multicast etc;

3.1.55.3.7. Deve exibir o status de dispositivos e da interface usando cores diferentes para representar status de aviso e críticos;

3.1.55.3.8. Deve monitorar a integridade do hardware de fornecedores populares como Cisco, DELL, F5, Juniper, HP etc. e deve permitir emissão de alertas e relatórios sobre o monitoramento da integridade do hardware;

3.1.55.3.9. Deve mostrar detalhes, tanto em tempo real quanto históricos, na forma de gráficos ecom a opção de escolha de períodos de tempo;

3.1.55.3.10. Deve ser capaz de descobrir e monitorar tanto dispositivos IPv4 quanto

IPv6;3.1.55.3.11. Deve ter opções de sondagem usando SNMP v1, v2c e v3 e WMI;

3.1.55.3.12. Deve ter opções para configurar os intervalos de sondagem, conforme necessário;

3.1.55.3.13. Deve ter opções para especificar períodos de retenção de dados;

3.1.55.3.14. Deve ter a opção para determinar a disponibilidade dos dispositivos usando somente SNMP;

3.1.55.3.15. A solução de monitoramento proposta deve ser capaz de descobrir dispositivos na redeautomaticamente com recursos SNMP e ICMP, mediante o fornecimento de:

3.1.55.3.15.1. intervalos de endereços

IP;3.1.55.3.15.2. sub-redes;

3.1.55.3.15.3. endereços IP

individuais;3.1.55.3.15.4. Active

Directory;

3.1.55.3.16. A solução não deve adicionar dispositivos com vários endereços IP como nós duplicados, mas relacionar todos os endereços IP conhecidos do nó;

3.1.55.3.17. Deve permitir a filtragem da interface quanto aos resultados da descoberta para excluir interfaces e portas de acesso virtuais e selecionar interfaces com base na correspondência de padrões;

3.1.55.3.18. Deve ter a opção de automatizar e agendar o processo de

descoberta; 3.1.55.3.19. Deve ser capaz de importar automaticamente

dispositivos descobertos;3.1.55.3.20. Deve sinalizar na console a descoberta

de novos dispositivos na rede; 3.1.55.3.21. Deve usar informações descobertas

para criar mapas de topologia;

3.1.55.3.22. A solução de gerenciamento proposta deve fornecer uma interface gráfica de usuário de alta qualidade com atualização assíncrona da exibição;

3.1.55.3.23. Deve fornecer uma visão unificada de alertas, interceptações, eventos, mensagensSyslog em uma única página;

3.1.55.3.24. Deve oferecer uma única visão unificada de informações de multicast, informações derotas e informações de dispositivo de um dispositivo;

3.1.55.3.25. Deve realçar rapidamente dispositivos com problemas, com base em diferentes propriedades, como tempo de resposta, carga da CPU, uso de memória, alto uso da interface etc.;

3.1.55.3.26. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em dispositivos ou interfaces (ou seja, seu acesso deve ser baseado em funções);

3.1.55.3.27. Deve registrar no console Web, para fins de auditoria, ações de usuários e eventos,que devem ficar disponíveis para emissão de alertas e relatórios;

3.1.55.3.28. Deve permitir a elaboração interativa de gráficos de nó, interface, volume etc.;

3.1.55.3.29. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável em um formato tabular;

3.1.55.3.30. Deve integrar-se ao Active Directory para fins de login de usuários;

3.1.55.3.31. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;

3.1.55.3.32. Deve ser capaz de gerar/criar o relatório via console Web;

3.1.55.3.33. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;

3.1.55.3.34. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definição de filtros, especificação de períodos de tempo, agrupamento de colunas etc;

3.1.55.3.35. Deve permitir a personalização avançada pelo fornecimento de opções para inserir consultas personalizadas diretas ao banco de dados;

3.1.55.3.36. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá -los no console Web;

3.1.55.3.37. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;

3.1.55.3.38. Deve permitir o envio por e-mail de painéis criados no console Web;

3.1.55.3.39. Deve ser capaz de configurar tanto gráficos quanto tabelas em um único relatório;

3.1.55.3.40. Deve ter opções para importar/exportar relatórios criados por outros usuários;

3.1.55.3.41. A solução de monitoramento proposta deve ser capaz de gerenciar e exibir

eventos

/alertas no console Web;

3.1.55.3.42. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;

3.1.55.3.43. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;

3.1.55.3.44. Deve permitir a inserção de consultas personalizadas para criar regras a serem aplicadas ao banco de dados;

3.1.55.3.45. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;

3.1.55.3.46. Deve permitir a criação de alertas com base em estados sustentados;

3.1.55.3.47. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e- mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da Web por e-mail etc.;

3.1.55.3.48. Deve ter a capacidade de estabelecer dinamicamente a linha de base de estatísticas e definir automaticamente o limite de alertas críticos e de aviso;

3.1.55.3.49. Deve permitir a supressão de alertas durante a manutenção programada;

3.1.55.3.50. A solução de monitoramento proposta deve permitir o agrupamento de dispositivos segundo diversas propriedades:

3.1.55.3.50.1. por departamento;

3.1.55.3.50.2. por local;

3.1.55.3.50.3. por nome;

3.1.55.3.50.4. por outras propriedades coletadas;

3.1.55.3.51. Deve ser capaz de definir dependências e relacionamentos entre dispositivos conectados e interfaces para evitar alertas de falso positivo por e-mail em caso de interrupção;

3.1.55.3.52. A solução de monitoramento proposta deve ser capaz de representar a rede pictoricamente e exibir detalhes de desempenho de dispositivos em tempo real;

3.1.55.3.53. Deve permitir a personalização de planos de fundo, ícones etc. e deve permitir que vários mapas de rede sejam aninhados com recurso de busca detalhada;

3.1.55.3.54. Deve ser capaz de exibir não apenas o status do dispositivo no mapa, mas também o status de qualquer outro detalhe obtido por meio da sondagem MIB personalizada;

3.1.55.3.55. Deve ter a capacidade de exibir o status de nós ou de um grupo agregado de nós por meio de dados dinamicamente atualizados;

3.1.55.3.56. Deve ser capaz de conectar dispositivos automaticamente por meio de informações de topologia reunidas durante a descoberta, como Cisco Discovery Protocol ou Link Layer Discovery Protocol;

3.1.55.3.57. Deve ser capaz de exibir a topologia multicast usando informações das listas de dispositivos upstream e downstream;

3.1.55.3.58. Deve ser capaz de exibir a localização geográfica de dispositivos;

3.1.55.3.59. Os dispositivos descobertos devem ser detectados como sendo de um fornecedor específico e categorizados automaticamente;

3.1.55.3.60. A solução de monitoramento proposta deve permitir a reunião de propriedades personalizadas de dispositivos habilitados para SNMP ao especificar o OID das propriedades;

3.1.55.3.61. Deve ser capaz de obter propriedades de dispositivos sem a necessidade de importar

MIBs de dispositivos para o banco de dados MIB;

3.1.55.3.62. Deve ser capaz de obter, em tempo real, valores, gráficos e alertas dessas propriedades personalizadas;

3.1.55.3.63. Deve ter APIs disponíveis para importar/exportar nós programaticamente e executar funcionalidades semelhantes;

3.1.55.3.64. Deve ser capaz de fornecer o Tempo de resposta da rede (NRT) e o Tempo deresposta do aplicativo (ART) de aplicativos críticos;

3.1.55.3.65. Deve contar com identificação e classificação pronta para uso de ~1.200 aplicativos;

3.1.55.3.66. Deve ter a capacidade de exibir métricas de volumes agregados por aplicativo/nó;

3.1.55.3.67. Deve ser capaz de fornecer contextualmente dados QoE de nós na sub exibição Detalhes do nó;

3.1.55.3.68. Deve ter utilitários para exibir o banco de dados e para interromper e iniciar serviços deaplicativos;

3.1.55.3.69. Deve ter opções para receber, exibir e gerar alertas de interceptações e mensagens Syslog de dispositivos;

3.1.55.3.70. Deve ter a opção de criação de relatórios sem fio para exibir pontos de acesso sem fiofinos e autônomos e seus clientes associados;

3.1.55.3.71. Deve ter exibições móveis personalizadas do console para visualização imediata por administradores;

3.1.55.3.72. Deve ser capaz de monitorar switches, pilha de energia e anéis de pilha de dados demembros individuais nas pilhas de switches da Cisco;

3.1.55.3.73. Deve ser capaz de criar relatórios sobre tecnologias como Cisco UCS, recurso

Energywise;

3.1.55.3.74. Deve ser capaz de criar relatórios sobre switches Cisco Nexus 1000V virtualizados,VSAN, switches Fibre Channel, como dispositivos Cisco MDS, Brocade, McData;

3.1.55.3.75. Deve ser capaz de monitorar toda a infraestrutura virtual VMware e Hyper-V, incluindo centrais virtuais, datacenters e clusters ESX, bem como rastrear automaticamente o desempenho das VMs;

3.1.55.3.76. Deve ser capaz de monitorar componentes individuais no ambiente de balanceamento de carga F5 BIG-IP;

3.1.55.3.77. Deve ser capaz de monitorar componentes individuais no firewall Cisco ASA, incluindo, entre outros, contagem de conexões, túneis VPN entre sites e por acesso remoto, identidade e utilização de interfaces, status de alta disponibilidade e status de sincronização de configuração.;

3.1.55.3.78. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;

3.1.55.3.79. Deve permitir a integração com aplicativos de terceiros na camada de interface do usuário, por meio de troca de mensagens e também de APIs;

3.1.55.3.80. A solução de monitoramento proposta deve ser capaz de acomodar o crescimento da rede pela adição de aplicativos de balanceamento de carga;

3.1.55.3.81. Deve permitir que informações de várias instâncias do aplicativo sejam consolidadas em uma única exibição;

3.1.55.4. Monitoramento de largura de banda:

3.1.55.4.1. A solução de monitoramento proposta deve ser capaz de monitorar o tráfego de redepela captura de dados de fluxo de dispositivos de rede, incluindo Cisco NetFlow v5 ou v9,

Juniper J- Flow, IPFIX, sFlow, dados de NetStream, amostras de dados de NetFlow e Cisco ASA NetFlow;

3.1.55.4.2. Deve identificar quais usuários, aplicativos e protocolos estão consumindo mais largura de banda;

3.1.55.4.3. Deve realçar os endereços IP dos principais consumidores de largura de banda na redee descobrir o uso indesejado de largura de banda;

3.1.55.4.4. Deve ser capaz de associar o tráfego vindo de diferentes fontes a nomes de aplicativos;

3.1.55.4.5. Deve ser capaz de receber fluxos de dispositivos que não estejam habilitados para SNMP, como VMware vSwitch;

3.1.55.4.6. Deve monitorar a qualidade de serviço baseada em classe (CBQoS) para descobrir seas políticas de priorização de tráfego são eficazes e se os aplicativos críticos para o negócio têm prioridade no tráfego da rede;

3.1.55.4.7. Também deve dar suporte às políticas de CBQoS aninhado;

3.1.55.4.8. Deve monitorar Tipo de serviço (ToS), Ponto de código diferenciado de serviços (DSCP)e Comportamento por salto (PHB);

3.1.55.4.9. Deve monitorar informações de BGP;

3.1.55.4.10. Deve mostrar detalhes tanto recentes quanto históricos na forma de gráficos com a opção de escolha de períodos de tempo;

3.1.55.4.11. Deve ter opções para especificar períodos de retenção de dados para evitar tensão no banco de dados e nos recursos de servidor;

3.1.55.4.12. Deve fornecer análise de fluxo com granularidade de um minuto e dar suporte a um fluxo sustentado de 60k por segundo;

3.1.55.4.13. A solução de monitoramento proposta deve ser capaz de adicionar automaticamente fontes de fluxo cujo desempenho já esteja sendo monitorado;

3.1.55.4.14. Deve notificar os fluxos que chegam de dispositivos e/ou interfaces não gerenciados e permitir sua adição para monitoramento com mínimo esforço;

3.1.55.4.15. A solução de gerenciamento proposta deve fornecer uma interface gráfica de usuário de alta qualidade;

3.1.55.4.16. Deve fornecer diversas exibições, categorizadas por usuário, aplicativo, departamento, conversa, interface, protocolo, tipo de serviço, Redes de sistemas autônomos;

3.1.55.4.17. Deve permitir a criação de exibições personalizadas do tráfego de rede, fornecendouma lista de parâmetros para seleção na definição de filtros;

3.1.55.4.18. Deve ter a capacidade de salvar exibições filtradas personalizadas como novos links na página da Web para facilitar o acesso posteriormente, com opções para pesquisar intervalos IP

/CIDR etc.;

3.1.55.4.19. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável em um formato tabular;

3.1.55.4.20. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em dispositivos ou interfaces (ou seja, seu acesso deve ser baseado em funções);

3.1.55.4.21. Deve integrar-se ao Active Directory para fins de login de usuários;

3.1.55.4.22. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;

3.1.55.4.23. Relatórios de qualidade de serviço baseada em classe devem fornecer detalhes sobre Pré-política, Pós-política e Abandonos;

3.1.55.4.24. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;

3.1.55.4.25. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definição de filtros, especificação de períodos de tempo, agrupamento de colunas etc;

3.1.55.4.26. Deve permitir a personalização avançada pelo fornecimento de opções para inserir consultas SQL diretas ao banco de dados;

3.1.55.4.27. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá -los no console Web;

3.1.55.4.28. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;

3.1.55.4.29. Deve permitir o envio por e-mail de painéis criados no console Web;

3.1.55.4.30. A solução de monitoramento proposta deve ser capaz de exibir eventos e alertas no console Web;

3.1.55.4.31. Alertas de qualidade de serviço baseada em classe (CBQoS) devem ser acionados quando o tráfego processado exceder os limites definidos para Pré-política, Pós-política e Abandonos.;

3.1.55.4.32. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;

3.1.55.4.33. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;

3.1.55.4.34. Deve permitir a inserção de consultas SQL para criar regras a serem aplicadas ao banco de dados;

3.1.55.4.35. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;

3.1.55.4.36. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e- mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da Web por e-mail etc.;

3.1.55.4.37. A solução de monitoramento proposta deve permitir a criação de grupos de endereços IP personalizados para categorizar fluxos por região, departamento, tipo de dispositivo etc.;

3.1.55.4.38. Deve ser capaz de usar esses grupos ao criar exibições personalizadas do tráfego de rede;

3.1.55.4.39. Deve ser capaz de fornecer uma visão resumida unificada levando em conta todos os dispositivos monitorados de diferentes fornecedores;

3.1.55.4.40. A solução de monitoramento proposta deve permitir a reunião de informações de fluxo de dispositivos que não sejam capacitados para fluxo quando usados com exportadores de fluxo de terceiros;

3.1.55.4.41. Deve ajudar na localização e no isolamento de computadores infectados em caso de ataque por vírus;

3.1.55.4.42. Deve dar importância às conversas com uso intensivo de banda larga para melhorar o desempenho do banco de dados, reduzir os tempos de carregamento de páginas e aumentar a velocidade de criação de relatórios;

3.1.55.4.43. Deve permitir a resolução de DNS e NetBIOS de nomes de domínio de pontos de extremidade;

3.1.55.4.44. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;

3.1.55.4.45. Deve permitir a integração com aplicativos de terceiros na camada de interface do usuário, por meio de troca de mensagens e também de APIs;

3.1.55.4.46. A solução de monitoramento proposta deve ser capaz de monitorar até 3 milhões de fluxos por segundo, devendo empregar métodos avançados de otimização;

3.1.55.4.47. Deve ser capaz de acomodar o crescimento da rede pela adição de aplicativos de balanceamento de carga;

3.1.55.4.48. Deve permitir que informações de várias instâncias do aplicativo sejam consolidadas em uma única exibição;

3.1.55.5. Gerenciamento de configurações:

3.1.55.5.1. A solução de gerenciamento proposta deve ser capaz de fazer automaticamente o backup da configuração (tanto de arquivos de configuração baseados em texto quanto binários) em roteadores, switches, firewalls, pontos de acesso e outros dispositivos de rede;

3.1.55.5.2. Deve ser capaz de fazer alterações em massa a configurações. Por exemplo, alterar cadeias de caracteres comunitárias, atualizar ACLs etc. em vários dispositivos;

3.1.55.5.3. Deve enviar alertas em tempo real quando acontecerem alterações à configuração da rede, com a comparação de quais linhas de configuração foram adicionadas, excluídas ou modificadas;

3.1.55.5.4. Deve permitir a comparação de arquivos de configuração de inicialização e execução para solucionar problemas de configuração de dispositivos;

3.1.55.5.5. Deve permitir a comparação da configuração atual com a do passado para permitir o entendimento das alterações que aconteceram ao longo do tempo;

3.1.55.5.6. Deve ajudar a automatizar tarefas repetidas pela definição de séries de comandos como modelos e sua execução com ou sem parâmetros;

3.1.55.5.7. Deve detectar violações da política de configuração para garantir a conformidade com regulamentações federais e padrões corporativos;

3.1.55.5.8. Deve automatizar o processo de aprovação de alterações permitindo ao administrador avaliar as alterações enviadas por carregadores antes de serem executadas nos dispositivos;

3.1.55.5.9. Deve fornecer um inventário do hardware de dispositivos de rede e contar com relatóriosprontos para uso de ativos e números de série;

3.1.55.5.10. Deve manter os dispositivos atualizados como parte da contratação e manutenção comrastreamento de suporte e fim da vida útil;

3.1.55.5.11. Deve ser compatível com vários protocolos, incluindo SNMP v1/v2c/v3, Telnet, SSH v1

/v2 e TFTP;

3.1.55.5.12. Deve permitir a especificação de informações de login, protocolos de transferência e portas de transferência nos níveis global e de dispositivo;

3.1.55.5.13. A solução de gerenciamento proposta deve ser capaz de descobrir dispositivos narede, mediante o fornecimento de:

3.1.55.5.13.1. intervalos de endereços

IP;3.1.55.5.13.2. sub-redes;

3.1.55.5.13.3. endereços IP individuais

3.1.55.5.14. Deve ter a opção de habilitar/desabilitar a adição automática dos nós descobertos;

3.1.55.5.15. Deve fornecer informações de Fim da vida útil/Fim do suporte (EoL/EoS) para ajudar amanter os dispositivos atualizados com relação à contratação e manutenção da implantação;

3.1.55.5.16. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável em um formato tabular;

3.1.55.5.17. Deve permitir o acesso remoto a recursos e funções relacionados a trabalhos, devendo também permitir o acesso remoto para atualizar configurações de dispositivos;

3.1.55.5.18. Deve fornecer seções separadas para tarefas de gerenciamento de configuração, inventário e relatórios sobre violações das políticas;

3.1.55.5.19. Deve realçar rapidamente dispositivos com violações da políticas, dispositivos cujo backup da configuração não tenha sido feito, dispositivos com conflitos na configuração etc;

3.1.55.5.20. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em dispositivos ou interfaces (ou seja, seu acesso deve ser baseado em funções);

3.1.55.5.21. Deve integrar-se ao Active Directory para fins de login de usuários;

3.1.55.5.22. A solução de gerenciamento proposta deve fornecer relatórios prontos para uso de diversas estatísticas monitoradas;

3.1.55.5.23. Deve ter relatórios de políticas criados para regulamentações especificadas em HIPAA, SOX, CISCP, Cisco Security Audit etc.

3.1.55.5.24. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definiçãode filtros, especificação de períodos de tempo, agrupamento de colunas etc;

3.1.55.5.25. Deve permitir que os relatórios sejam enviados de acordo com programações diárias,semanais e mensais;

3.1.55.5.26. Deve permitir o envio por e-mail de painéis criados no console Web;

3.1.55.5.27. A solução de gerenciamento proposta deve ser capaz de exibir eventos e alertas no console Web;

3.1.55.5.28. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;

3.1.55.5.29. Deve ser capaz de fazer backup da configuração, executar o script de configuração, mostrar alterações à última configuração como ações de alertas;

3.1.55.5.30. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e- mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da Web por e-mail etc.;

3.1.55.5.31. A solução de gerenciamento proposta deve permitir o agrupamento de dispositivossegundo diversas propriedades:

3.1.55.5.31.1. por fornecedor;

3.1.55.5.31.2. tipo de

máquina;

3.1.55.5.31.3. imagem de sistema operacional;

3.1.55.5.31.4. versão do sistema operacional;

3.1.55.5.31.5. resultado do último login;

3.1.55.5.31.6. outras propriedades

personalizadas;

3.1.55.5.32. Os dispositivos descobertos devem ser detectados como sendo de um fornecedorespecífico e categorizados automaticamente;

3.1.55.5.33. A solução de gerenciamento proposta deve permitir a criação ou modificação de modelos de comandos para dispositivos que não contem com suporte pronto para uso;

3.1.55.5.34. Deve permitir a criação de modelos de dispositivos personalizados para automatizar tarefas de configuração repetidas;

3.1.55.5.35. Deve ser capaz de criar relatórios de políticas personalizados especificando o conteúdo que deve ou não estar presente na configuração. O conteúdo pode ser especificado como uma sequência de caracteres ou uma expressão regular;

3.1.55.5.36. Deve ter opções para receber, exibir e gerar alertas de interceptações e mensagens Syslog de dispositivos;

3.1.55.5.37. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;

3.1.55.5.38. A solução de gerenciamento proposta deve ser capaz de gerenciar até 10.000 dispositivos e acomodar o crescimento da rede pela adição de aplicativos de balanceamento de carga;

3.1.55.6. Monitoramento de WAN e VOIP:

3.1.55.6.1. A solução de monitoramento proposta deve ser capaz de identificar problemas de desempenho de rede específicos a sites ou relacionados à WAN usando a tecnologia Cisco IP

SLA, além de monitorar caminhos de chamada VoIP para garantir a qualidade do serviço do tráfego de voz;

3.1.55.6.2. Deve fornecer automaticamente estatísticas aprofundadas de desempenho de VoIP em tempo real, incluindo MOS, tremulação, latência de rede e perda de pacotes;

3.1.55.6.3. Deve ajudar a determinar o impacto do desempenho da WAN nos principais aplicativos;

3.1.55.6.4. Deve exibir o status de operações IP SLA usando cores diferentes para representar status de aviso e críticos;

3.1.55.6.5. Deve monitorar dados CDR/CMR para monitoramento de qualidade de chamada em tempo real e coleta de dados granulares, além de usar esses dados em alertas e relatórios;

3.1.55.6.6. Deve ajudar a pesquisar chamadas VoIP e exibir detalhes de chamadas VoIP, chamadas com falha, chamadas da região, detalhes da região, causas de desconexão, chamadas por região, detalhes de telefone VoIP, detalhes do caminho, detalhes de gateway/ponto de extremidade VoIP etc.;

3.1.55.6.7. Deve ter opções para pesquisar registros de chamadas VoIP para localizar e solucionar problemas de chamadas problemáticas;

3.1.55.6.8. Deve fazer o monitoramento em tempo real da utilização de troncos PRI VoIP em gateways PRI da Cisco, fornecendo interface do usuário de distribuição de dados, gráficos de utilização de troncos e estatísticas históricas de utilização de VoIP e dados de gateways;

3.1.55.6.9. Deve mostrar detalhes, tanto em tempo real quanto históricos, na forma de gráficos ecom a opção de escolha de períodos de tempo;

3.1.55.6.10. Deve ter opções para configurar os intervalos de sondagem, conforme

necessário;3.1.55.6.11. Deve ter opções para especificar períodos de retenção de dados;

3.1.55.6.12. A solução de monitoramento proposta deve ser capaz de descobrir dispositivos capacitados para IP SLA e fornecer a opção de adicioná-los diretamente ao monitoramento;

3.1.55.6.13. Esse console Web deve mostrar detalhes de gateways, como principais problemas de qualidade de chamadas de cada gateway, lista de todas as chamadas com falhas relacionadas a um gateway e utilização percentual atual de cada tronco;

3.1.55.6.14. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável em um formato tabular;

3.1.55.6.15. Deve permitir a personalização por contar com opções para adicionar/remover seçõesem página da Web, conforme necessário;

3.1.55.6.16. Deve realçar rapidamente operações com problemas, com base em diferentes propriedades, como latência, tremulação, MOS etc.;

3.1.55.6.17. Deve integrar-se ao Active Directory para fins de login de usuários

3.1.55.6.18. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;

3.1.55.6.19. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;

3.1.55.6.20. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definiçãode filtros, especificação de períodos de tempo, agrupamento de colunas etc.;

3.1.55.6.21. Deve permitir a personalização avançada pelo fornecimento de opções para inserir consultas SQL diretas ao banco de dados;

3.1.55.6.22. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá -los no console Web;

3.1.55.6.23. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;

3.1.55.6.24. Deve permitir o envio por e-mail de painéis criados no console Web;

3.1.55.6.25. A solução de monitoramento proposta deve ser capaz de exibir eventos e alertas no console Web;

3.1.55.6.26. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;

3.1.55.6.27. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;

3.1.55.6.28. Deve permitir a inserção de consultas SQL para criar regras a serem aplicadas ao banco de dados;

3.1.55.6.29. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;

3.1.55.6.30. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e- mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da Web por e-mail etc.;

3.1.55.6.31. A solução de monitoramento proposta deve permitir o agrupamento de dispositivos segundo diversas propriedades – por local, por departamento, por nome e por outras propriedades coletadas;

3.1.55.6.32. A solução de monitoramento proposta deve ser capaz de representar a rede pictoricamente e exibir detalhes de dispositivos e operações em tempo real;

3.1.55.6.33. Deve permitir a personalização de planos de fundo, ícones etc. e deve permitir que vários mapas de rede sejam aninhados com recurso de busca detalhada;

3.1.55.6.34. A solução de monitoramento proposta deve dar suporte a operações IP SLA populares, incluindo: HTTP, FTP, DNS, DHCP, Conexão TCP, Tremulação UDP, Tremulação VoIP UDP, Eco ICMP, Eco UDP, Eco de caminho ICMP, Tremulação de caminho ICMP;

3.1.55.6.35. Deve ter utilitários para exibir o banco de dados e para interromper e iniciar serviços de aplicativos; 3.1.55.6.36. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;

3.1.55.6.37. A solução de monitoramento proposta deve ser capaz de acomodar novos locais pela adição de aplicativos de balanceamento de carga;

3.1.55.7. Gerenciamento de endereços IP, DNS, DHCP:

3.1.55.7.1. A solução de monitoramento proposta deve ser capaz de gerenciar tarefas e conflitos de espaços de endereços IP usando uma interface do usuário centralizada baseada na Web;

3.1.55.7.2. Deve emitir um alerta antes do preenchimento de uma sub-rede ou escopo de DHCP;
3.1.55.7.3. Deve verificar endereços IP automaticamente e atualizar seu status;

3.1.55.7.4. Deve mostrar quais sub-redes estão próximas à capacidade total e como estão

alocadas;3.1.55.7.5. Deve permitir a definição de grupos e de segmentações para verificação;

3.1.55.7.6. Deve alocar automaticamente sub-redes corretamente dimensionadas especificando ostamanhos de super-redes e sub-redes;

3.1.55.7.7. Deve ter detecção ativa de conflitos de endereços IP, tanto em ambientes estáticosquanto DHCP;

3.1.55.7.8. Deve rastrear endereços IP historicamente e mostrar a alteração das propriedades ao longo do tempo;

3.1.55.7.9. Deve rastrear endereços IPv4 e IPv6 pela execução de uma pesquisa global;

3.1.55.7.10. Deve dar suporte ao gerenciamento e monitoramento de BIND DNS, permitindo acriação, modificação e exclusão de zonas DNS e registros DNS do BIND DNS v8.x, v9.x e v9.11+;

3.1.55.7.11. Deve monitorar o status do serviço BIND DNS e o status das

zonas;3.1.55.7.12. Deve ajudar no planejamento da migração para IPv6;

3.1.55.7.13. Deve permitir servidores DHCP de vários fornecedores – Windows, Cisco IOS e ISC;

3.1.55.7.14. A solução de monitoramento proposta deve permitir a importação de endereços IP a partir de planilhas;

3.1.55.7.15. Deve permitir a adição em massa de sub-redes, adicionando servidores DHCP e servidores DNS;

3.1.55.7.16. Deve usar o Microsoft Active Directory para fazer login no console Web;

3.1.55.7.17. Deve permitir a personalização por contar com opções para adicionar/remover seçõesem página da Web, conforme necessário;

3.1.55.7.18. Deve realçar rapidamente dispositivos com problemas, como os que apresentam umaalta porcentagem de portas utilizadas;

3.1.55.7.19. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em dispositivos ou interfaces (ou seja, seu acesso deve ser baseado em funções);

3.1.55.7.20. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;

3.1.55.7.21. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;

3.1.55.7.22. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definiçãode filtros, especificação de períodos de tempo, agrupamento de colunas etc.;

3.1.55.7.23. Deve permitir a personalização avançada pelo fornecimento de opções para inserirconsultas SQL diretas ao banco de dados;

3.1.55.7.24. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá -los no console Web;

3.1.55.7.25. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;

3.1.55.7.26. Deve permitir o envio por e-mail de painéis criados no console Web;

3.1.55.7.27. A solução de monitoramento proposta deve ser capaz de exibir eventos e alertas no console Web;

3.1.55.7.28. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;

3.1.55.7.29. Deve alertar quando houver um conflito de endereços IP com base no endereço MAC, quando os escopos DHCP se sobrepuserem a um endereço IP existente, quando houver uma alta utilização de sub-redes etc.;

3.1.55.7.30. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;

3.1.55.7.31. Deve permitir a inserção de consultas SQL para criar regras a serem aplicadas ao banco de dados;

3.1.55.7.32. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;

3.1.55.7.33. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de

e- mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da Web por e-mail etc.;

3.1.55.7.34. A solução de monitoramento proposta deve permitir o agrupamento de dispositivos segundo diversas propriedades:

3.1.55.7.34.1. por departamento;

3.1.55.7.34.2. por local;

3.1.55.7.34.3. por nome;

3.1.55.7.34.4. e por outras propriedades coletadas;

3.1.55.7.35. Deve permitir a adição dinâmica de membros a grupos pela especificação de uma propriedade capaz de alterar valores dinamicamente, como volumes que estejam ficando com pouco espaço livre;

3.1.55.7.36. Deve ser capaz de definir relacionamentos entre dispositivos conectados e interfaces para evitar alertas de falso positivo por e-mail em caso de interrupção;

3.1.55.7.37. A solução de monitoramento proposta não deve ser específica a um fornecedor;

3.1.55.7.38. A solução de monitoramento proposta deve ser capaz de localizar todos os pontos de extremidade em uma sub-rede;

3.1.55.7.39. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;

3.1.55.7.40. Deve integrar-se ao software de monitoramento de portas para mostrar informações de portas e usuários juntamente com o histórico de hosts de endereços IP ou de atribuição de DNS;

3.1.55.7.41. Deve permitir o desligamento remoto de portas em caso de conflitos de endereços IPdevido à integração;

3.1.55.7.42. Deve fornecer um pacote VMO para integrar-se ao VMware vRealize Orchestrator paraproporcionar automação do fluxo de trabalho:

3.1.55.7.42.1. Simplificar o gerenciamento de endereços IP nas VMs;

3.1.55.7.42.2. Automatizar o provisionamento de endereços IP às VMs;

3.1.55.7.42.3. Automatizar o monitoramento de registros DNS das VMs;

3.1.55.7.43. Deve fornecer APIs para integração com produtos de

terceiros;

3.1.55.7.44. A solução de monitoramento proposta deve ser capaz de acomodar o crescimento darede pela adição de aplicativos de balanceamento de carga;

3.1.55.8. Monitoramento de portas de Switch:

3.1.55.8.1. A solução de monitoramento proposta deve ser capaz de rastrear a localização atual deum dispositivo ao obter seu endereço IP, nome de host ou endereço MAC;

3.1.55.8.2. Deve ajudar a localizar dispositivos invasores de maneira fácil e

rápida;3.1.55.8.3. Deve localizar portas de rede disponíveis;

3.1.55.8.4. Deve alertar quando um dispositivo específico se conecta, observando seu endereçoMAC ou nome de host;

3.1.55.8.5. Deve mostrar as últimas localizações conhecidas (switch e porta) de um dispositivodesconectado;

3.1.55.8.6. Deve descobrir switches que estejam funcionando próximo da capacidade máxima parajustificar a compra de novos equipamentos;

3.1.55.8.7. Deve mostrar cada porta de um switch para recuperar portas que não estejam em uso;

3.1.55.8.8. Deve monitorar os controladores quanto a pontos de acesso sem fio e pontos de acessodinâmicos conectados a tais controladores;

3.1.55.8.9. Deve ter a opção de configurar uma lista branca de dispositivos com base em endereçoMAC, endereço IP ou nome de host;

3.1.55.8.10. Deve sondar dispositivos quanto a dados de

VRF;3.1.55.8.11. Deve ter a opção de desligar portas

remotamente;

3.1.55.8.12. Deve permitir a adição de um controlador de domínio do Active Directory para rastreara atividade de logon na rede de usuários associados ao Active Directory;

3.1.55.8.13. Deve facilitar a coleta de informações de login de usuário configurando o nível deregistro em log apropriado nos servidores Windows;

3.1.55.8.14. Deve ser capaz de rastrear clientes VPN conectados ao Cisco ASA;

3.1.55.8.15. A solução de monitoramento proposta deve ser capaz de descobrir dispositivos, bem como de descobrir portas nesses dispositivos;

3.1.55.8.16. Deve ter opções de filtragem avançadas durante a descoberta de portas (como filtragem baseada em status, tronco, intervalo de portas, VLAN etc.) para reduzir o número de portas que precisam ser ativamente monitoradas;

3.1.55.8.17. A solução de gerenciamento proposta deve fornecer uma interface gráfica de usuário de alta qualidade;

3.1.55.8.18. Deve permitir a personalização por contar com opções para adicionar/remover seções em página da Web, conforme necessário;

3.1.55.8.19. Deve realçar rapidamente dispositivos com problemas, como os que apresentam uma alta porcentagem de portas utilizadas;

3.1.55.8.20. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em dispositivos ou interfaces (ou seja, seu acesso deve ser baseado em funções);

3.1.55.8.21. Deve integrar-se ao Active Directory para fins de login de usuários;

3.1.55.8.22. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;

3.1.55.8.23. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;

3.1.55.8.24. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definição de filtros, especificação de períodos de tempo, agrupamento de colunas etc.;

3.1.55.8.25. Deve permitir a personalização avançada pelo fornecimento de opções para inserir consultas SQL diretas ao banco de dados;

3.1.55.8.26. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá -los no console Web;

3.1.55.8.27. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais; 3.1.55.8.28. Deve permitir o envio por e-mail de painéis criados no console Web;

3.1.55.8.29. A solução de monitoramento proposta deve ser capaz de exibir eventos e alertas no console Web;

3.1.55.8.30. As informações de alertas e eventos devem ser registradas no banco de dados para

referência futura;

3.1.55.8.31. Deve alertar quando um novo endereço MAC aparece na rede, quando aparece um nome de host na rede que não consta da lista branca e quando um item que está sendo observado fica ativo;

3.1.55.8.32. Deve alertar quando um ponto de extremidade é alterado;

3.1.55.8.33. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;

3.1.55.8.34. Deve permitir a inserção de consultas SQL para criar regras a serem aplicadas ao banco de dados;

3.1.55.8.35. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;

3.1.55.8.36. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e- mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da Web por e-mail etc.;

3.1.55.8.37. A solução de monitoramento proposta deve permitir o agrupamento de dispositivos segundo diversas propriedades:

3.1.55.8.37.1. por departamento;

3.1.55.8.37.2. por local;

3.1.55.8.37.3. por nome;

3.1.55.8.37.4. e por outras propriedades coletadas;

3.1.55.8.38. Deve permitir a adição dinâmica de membros a grupos pela especificação de uma

propriedade capaz de alterar valores dinamicamente, como volumes que estejam ficando com pouco espaço livre;

3.1.55.8.39. Deve ser capaz de definir relacionamentos entre dispositivos conectados e interfaces para evitar alertas de falso positivo por e-mail em caso de interrupção;

3.1.55.8.40. A solução de monitoramento proposta não deve ser específica a um fornecedor;

3.1.55.8.41. Os dispositivos descobertos devem ser detectados como sendo de um fornecedor específico e categorizados automaticamente;

3.1.55.8.42. A solução de monitoramento proposta deve ser capaz de localizar todos os pontos de extremidade em uma sub-rede;

3.1.55.8.43. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;

3.1.55.8.44. A solução de monitoramento proposta deve ser capaz de acomodar o crescimento da rede pela adição de aplicativos de balanceamento de carga;

3.1.55.9. Monitoramento de aplicativos:

3.1.55.9.1. A solução de monitoramento proposta deve ser capaz de

monitorar:3.1.55.9.1.1. Status de aplicativos;

3.1.55.9.1.2. Estatísticas de desempenho de

aplicativos;3.1.55.9.1.3. Serviços e processos;

3.1.55.9.1.4. Desempenho do sistema

operacional;3.1.55.9.1.5. Hardware;

3.1.55.9.2. Deve fornecer automaticamente uma visão em tempo real dos processos em execuçãonos sistemas e estatísticas aprofundadas do desempenho de aplicativos após sua

descoberta

/configuração;

3.1.55.9.3. Deve ser capaz de gerenciar processos, serviços em execução nos sistemas e estatísticas aprofundadas do desempenho de aplicativos após sua descoberta/configuração;

3.1.55.9.4. Deve fornecer automaticamente uma visão em tempo real de logs de eventos do Windows, incluindo o nível dos logs de eventos, a identificação do evento e sua fonte;

3.1.55.9.5. Deve ter métodos de monitoramento especializados que indicam o status e o desempenho dos principais parâmetros dos aplicativos (como serviços, comprimento da fila no caso do Exchange, consultas SQL no caso de bancos de dados etc.) com base em práticas recomendadas;

3.1.55.9.6. Deve ser capaz de reunir importantes parâmetros de um aplicativo em um único modelo de monitoramento que possa ser uniformemente aplicado a aplicativos em diferentes servidores;

3.1.55.9.7. Uma personalização feita no modelo de monitoramento de um aplicativo deve ser propagada imediatamente para todos os outros servidores que tenham o aplicativo;

3.1.55.9.8. Deve permitir o uso de scripts personalizados com diversas opções de mecanismo de script, como VBscript, Perl, Powershell etc.;

3.1.55.9.9. Deve ter opções de monitoramento da experiência do usuário com diversos aplicativos e serviços, como HTTP, FTP, DHCP, DNS, SQL Server, Oracle, JSON, etc. para descobrir problemas, antes mesmo que os usuários se deem conta deles;

3.1.55.9.10. Deve ser capaz de criar relatórios com detalhes de hardware (como CPU, memória, estado de ventiladores, alimentação etc.) de servidores de fornecedores populares, como IBM, HP, DELL, bem como hosts VMware;

3.1.55.9.11. Deve ter opções de sondagem usando SNMP, WMI e outros métodos;

3.1.55.9.12. Deve exibir o status de aplicativos e de serviços importantes usando cores diferentes

para representar status de aviso e críticos;

3.1.55.9.13. Deve mostrar detalhes, tanto em tempo real quanto históricos, na forma de gráficos e com a opção de escolha de períodos de tempo;

3.1.55.9.14. Deve ter opções para configurar os intervalos de sondagem, conforme necessário;

3.1.55.9.15. Deve ser capaz de obter métricas de desempenho de E/S de disco de processos e serviços monitorados via WMI;

3.1.55.9.16. Deve ter opções para especificar períodos de retenção de dados;

3.1.55.9.17. Deve ser capaz de fornecer Registro em logs de eventos de auditoria de usuário, incluindo:

3.1.55.9.17.1. Processos encerrados;

3.1.55.9.17.2. Serviços parados / iniciados / reiniciados / Nós reinicializados;

3.1.55.9.17.3. Credenciais e gabaritos de aplicativos recém-criados / editados /

excluídos;3.1.55.9.17.4. Aplicativos atribuídos, removidos, gerenciados e não

gerenciados; 3.1.55.9.18. Deverá possuir recurso de monitoramento de nuvem para:

3.1.55.9.18.1. Descobrir e monitorar instâncias EC2 na nuvem via

API; 3.1.55.9.18.2. Descobrir e monitorar volumes EBS via API;

3.1.55.9.18.3. Descobrir e monitorar o serviço de nuvem via API;

3.1.55.9.18.4. Descobrir e monitorar novas instâncias

automaticamente;

3.1.55.9.18.5. Consolidar a exibição de sistemas em nuvem, híbridos e locais;

3.1.55.9.18.6. Monitorar o desempenho de aplicativos e métricas de sistema operacional em

instâncias na nuvem;

3.1.55.9.19. A solução de monitoramento proposta deve ser capaz de descobrir aplicativos nos servidores escolhidos, aplicar o monitoramento a eles e dar início a estatísticas para relatório em alguns minutos;

3.1.55.9.20. Deve ter uma opção para localizar processos por WMI ou SNMP, Monitores de contador de desempenho, Monitores WMI, Monitores de contador de desempenho do VMware etc.;

3.1.55.9.21. Deve ter uma opção para localizar monitores JMX para monitoramento de aplicativos baseados em Java, como JBoss, Tomcat, WebLogic etc.;

3.1.55.9.22. Deve ser capaz de descobrir servidores de e-mail e diretório, bancos de dados, serviços de rede, sistemas operacionais, servidores VMware ESX etc. automaticamente por meio de modelos de monitoramento incorporados;

3.1.55.9.23. Deve ser capaz de criar e definir o cálculo automático de limites críticos e de aviso a partir de dados de linha de base;

3.1.55.9.24. Deve fornecer monitoramento aprofundado (AppInsight) e pronto para uso do Microsoft SQL com o seguinte: Logs de erros SQL, Exibições individuais de detalhes de bancos de dados, Status de agente SQL, Resultados de trabalhos, Fragmentação de índices, Conexões de SQL Server;

3.1.55.9.25. Deve fornecer monitoramento aprofundado (AppInsight) de servidores de função de caixa de correio do Microsoft Exchange, incluindo desempenho do repositório de informações, banco de dados, armazenamento, replicação etc.;

3.1.55.9.26. Deve analisar as tendências de e-mails e anexos enviados e recebidos de cada usuário de caixa de correio;

3.1.55.9.27. Deve fornecer monitoramento aprofundado (AppInsight) do Microsoft Internet Information Service (IIS), incluindo serviços, processos, conexões com sites individuais e tempo de resposta, pool de aplicativos individuais e outras estatísticas, como cache e conexão.;

3.1.55.9.28. Deve fornecer monitoramento aprofundado de produtos do Microsoft Office 365, incluindo Caixas de correio do Exchange, tráfego de e-mail, segurança, status de assinaturas e estatísticas de dispositivos móveis;

3.1.55.9.29. A solução de gerenciamento proposta deve fornecer uma interface gráfica de usuário de alta qualidade;

3.1.55.9.30. Deve fornecer uma exibição unificada de alertas, interceptações, eventos etc. em uma única página;

3.1.55.9.31. Deve realçar rapidamente aplicativos com problemas, com base em diferentes propriedades, como:

3.1.55.9.31.1. aplicativos inativos;

3.1.55.9.31.2. aplicativos com

problemas;

3.1.55.9.31.3. parâmetros com alta utilização de

CPU;3.1.55.9.31.4. memória, etc;

3.1.55.9.32. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em aplicativos (ou seja, seu acesso deve ser baseado em funções);

3.1.55.9.33. Deve permitir a elaboração interativa de gráficos;

3.1.55.9.34. Deve integrar-se ao Active Directory para fins de login de usuários;

3.1.55.9.35. Deve ter opções de integração para visualizar automaticamente objetos relevantes da infraestrutura virtual, como repositórios de dados e objetos de armazenamento, como LUNs;

3.1.55.9.36. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável em um formato tabular;

3.1.55.9.37. Criação de relatórios avançada;

3.1.55.9.38. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;

3.1.55.9.39. Deve ser capaz de gerar/criar o relatório via console Web;

3.1.55.9.40. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;

3.1.55.9.41. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definição de filtros, especificação de períodos de tempo, agrupamento de colunas etc.;

3.1.55.9.42. Deve permitir a personalização avançada pelo fornecimento de opções para inserir consultas personalizadas diretas ao banco de dados;

3.1.55.9.43. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá -los no console Web;

3.1.55.9.44. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;

3.1.55.9.45. Deve permitir o envio por e-mail de painéis criados no console Web;

3.1.55.9.46. Deve ser capaz de configurar tanto gráficos quanto tabelas em um único relatório;3.1.55.9.47. Deve ter opções para importar/exportar relatórios criados por outros usuários; 3.1.55.9.48. Deve dar suporte a vários formatos, como PDF, HTML e CSV;

3.1.55.9.49. A solução de monitoramento proposta deve ser capaz de gerenciar e exibir eventos

/alertas no console Web;

3.1.55.9.50. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;

3.1.55.9.51. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;

3.1.55.9.52. Deve permitir a inserção de consultas personalizadas para criar regras a serem aplicadas ao banco de dados;

3.1.55.9.53. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;

3.1.55.9.54. Deve permitir a criação de alertas com base em estados sustentados;

3.1.55.9.55. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e- mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da Web por e-mail etc.;

3.1.55.9.56. Deve ter suporte a variáveis na mensagem de e-mail de alerta para tornar o conteúdo mais autoexplicativo;

3.1.55.9.57. A solução de monitoramento proposta deve permitir o agrupamento de aplicativos segundo diversas propriedades:

3.1.55.9.57.1. por departamento;

3.1.55.9.57.2. por local;

3.1.55.9.57.3. por nome;

3.1.55.9.57.4. e por outras propriedades coletadas;

3.1.55.9.58. Deve permitir a adição dinâmica de membros a grupos pela especificação de uma propriedade capaz de alterar valores dinamicamente, como volumes que estejam ficando com pouco espaço livre;

3.1.55.9.59. Deve ser capaz de definir relacionamentos entre servidores e aplicativos para evitar alertas de falso positivo por e-mail em caso de interrupção;

3.1.55.9.60. A solução de monitoramento proposta deve ser capaz de representar os aplicativos pictoricamente e exibir detalhes de desempenho de aplicativos em tempo real;

3.1.55.9.61. Deve permitir a personalização de planos de fundo, ícones etc. e deve permitir que vários mapas sejam aninhados com recurso de busca detalhada;

3.1.55.9.62. A solução de monitoramento proposta não deve ser específica a um aplicativo;

3.1.55.9.63. Os aplicativos descobertos devem ser monitorados com modelos de monitoramento incorporados criados com base em práticas recomendadas;

3.1.55.9.64. A solução de monitoramento proposta deve permitir a inclusão de scripts personalizados para estender os recursos de monitoramento dos aplicativos;

3.1.55.9.65. Deve ser capaz de obter, em tempo real, valores, gráficos e alertas dessas propriedades personalizadas;

3.1.55.9.66. Deve ter APIs disponíveis para importar/exportar nós programaticamente e executar funcionalidades semelhantes;

3.1.55.9.67. Deve ter utilitários para exibir o banco de dados e para interromper e iniciar serviços de aplicativos;

3.1.55.9.68. Deve ter exibições móveis personalizadas do console para visualização imediata por administradores;

3.1.55.9.69. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;

3.1.55.9.70. Deve integrar-se ao software de monitoramento de virtualização para oferecer uma exibição do desempenho do aplicativo de ponta a ponta, desde o aplicativo até a VM e o host.;

3.1.55.9.71. Deve permitir a integração com aplicativos de terceiros na camada de interface do usuário, por meio de troca de mensagens e também de APIs;

3.1.55.9.72. A solução de monitoramento proposta deve ser capaz de acomodar o crescimento pela adição de aplicativos de balanceamento de carga;

3.1.55.9.73. Deve permitir que informações de várias instâncias do aplicativo sejam consolidadas em uma única exibição;

3.1.55.10. Monitoramento de virtualização:

3.1.55.10.1. A solução de monitoramento proposta deve ser capaz de fazer o gerenciamento de hipervisores heterogêneos, como ambientes VMware vSphere e Microsoft Hyper-V, em um único local;

3.1.55.10.2. Deve fazer o monitoramento do desempenho de ambientes VMware, incluindo VMware ESX, vSphere, ESXi, vCenter Server;

3.1.55.10.3. Deve coletar informações de desempenho e capacidade de clusters, hosts e máquinas virtuais (VMs) no armazenamento do Hyper-V;

3.1.55.10.4. Deve fazer o monitoramento de desempenho e indicar problemas, como problemas de E/S de armazenamento;

3.1.55.10.5. Deve monitorar, detectar e solucionar problemas proativamente de afunilamentos de capacidade;

3.1.55.10.6. Deve possibilitar cenários hipotéticos e ajudar a determinar o posicionamento ideal de VMs;

3.1.55.10.7. Deve ajudar a planejar novas compras e identificar recursos super e

subutilizados;3.1.55.10.8. Deve ajudar a controlar a dispersão de VMs com análise

avançada;

3.1.55.10.9. Deve descobrir VMs ociosas/obsoletas, VMs zumbis, arquivos órfãos e VMs sobrecarregadas;

3.1.55.10.10. Deve ser capaz de rastrear configurações de VMs e hosts ao longo do tempo emostrar alterações à configuração ambiental;

3.1.55.10.11. Deve permitir a comparação de configurações ao longo do tempo e ajudar a ver exatamente quando uma configuração foi alterada, para ajudar acelerando e melhorando a solução de problemas;

3.1.55.10.12. Deve possibilitar a automação de estorno, identificar custos de nuvem e exibir showback;

3.1.55.10.13. Deverá possuir recursos de planejamento de capacidade, onde:

3.1.55.10.13.1. Fornece um assistente de cenário que ajuda a criar modelos de configuração deVMs e simula o cenário com base no histórico de desempenho, nas novas necessidades do sistema e nos recursos atualmente disponíveis;

3.1.55.10.13.2. Fornece recomendações preditivas para recursos de CPU, memória e armazenamento que usam padrões e tendências históricas;

3.1.55.10.13.3. Gera um relatório com estatísticas detalhadas de uso que abrangem consumo previsto de recursos e recomendações para atendimento de necessidades futuras;

3.1.55.10.13.4. Deve ser capaz de executar correções imediatamente ou em lotes, de acordo com aprogramação, com os dados fornecidos pelas recomendações automáticas;

3.1.55.10.14. Deve ser capaz de descobrir e monitorar instâncias EC2 na nuvem via API;

3.1.55.10.15. Deve ser capaz de descobrir e monitorar volumes EBS na nuvem via API;

3.1.55.10.16. Deve ser capaz de descobrir e monitorar o serviço de nuvem via API;

3.1.55.10.17. Deve ser capaz de descobrir e monitorar novas instâncias automaticamente;

3.1.55.10.18. Deve fornecer uma exibição consolidada de sistemas em nuvem, híbridos e

locais;

3.1.55.10.19. A solução de gerenciamento proposta deve fornecer uma interface gráfica de usuáriode alta qualidade;

3.1.55.10.20. Deve permitir a personalização por contar com opções para adicionar/remover widgets em página da Web, conforme necessário;

3.1.55.10.21. Deve permitir a criação de painéis personalizados para diferentes finalidades, comopainéis separados para monitoramento de desempenho, planejamento de capacidade, estorno etc.;

3.1.55.10.22. Deve ter opções de integração para visualizar automaticamente aplicativos relevantes e objetos de armazenamento, como LUNs, e integrá-los a objetos de infraestrutura virtual relevantes, como repositórios de dados e clusters;

3.1.55.10.23. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável em um formato tabular;

3.1.55.10.24. Deve fornecer uma interface para executar a correção em um único clique de problemas de recursos de VMs;

3.1.55.10.25. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;

3.1.55.10.26. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;

3.1.55.10.27. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;

3.1.55.10.28. Deve permitir o envio por e-mail de painéis criados no console Web;

3.1.55.10.29. A solução de monitoramento proposta deve ajudar a detectar rapidamente e tratar problemas de desempenho usando alertas flexíveis e recomendações integradas;

3.1.55.10.30. A solução de monitoramento proposta deve ser capaz de exibir eventos e alertas no console Web;

3.1.55.10.31. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;

3.1.55.10.32. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;

3.1.55.10.33. A solução de monitoramento proposta deve permitir o agrupamento de dispositivos segundo diversas propriedades:

3.1.55.10.33.1. por departamento;

3.1.55.10.33.2. por local;

3.1.55.10.33.3. por nome;

3.1.55.10.33.4. e por outras propriedades coletadas;

3.1.55.10.34. Deve ter recursos de pesquisa avançada para pesquisar, filtrar e classificar segundoos atributos de configuração e desempenho coletados;

3.1.55.10.35. Deve ser capaz de exibir relacionamentos entre recursos conectados ao longo do tempo para mapear as dependências entre os objetos do datacenter virtual, como VMs, hosts, repositórios de dados, clusters e vApps;

3.1.55.10.36. Deve ser capaz de obter propriedades de virtualização e personalizá-las em exibições de painéis por meio de recursos de pesquisa avançada;

3.1.55.10.37. Deve ser instalável em um ambiente VMware ou Hyper-V, devendo exigir apenas uma instalação para gerenciar um ambiente VMware e Hyper-V misto;

3.1.55.10.38. Deve integrar-se ao software de monitoramento de aplicativos para oferecer uma exibição do desempenho do aplicativo de ponta a ponta, desde o aplicativo até a VM e o host.;

3.1.55.10.39. Deve ajudar a identificar se o aplicativo está apresentando problemas devido à VM onde reside ou devido a outras VMs com alto consumo de recursos no mesmo recurso compartilhado;

3.1.55.10.40. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;

3.1.55.10.41. A solução de monitoramento proposta deve ser capaz de monitorar ambientes distribuídos em larga escala com mais de 10.000 VMs;

3.1.56. A solução deverá atender as métricas mínimas listadas abaixo:

3.1.56.1. Equipamentos de rede Links: Firewalls/Switches/WI-

FI:3.1.56.1.1. Consumo do Link;

3.1.56.1.2. Throughput;

3.1.56.1.3. Latência do Link;

3.1.56.1.4. Consumo de

Processador;3.1.56.1.5.

Disponibilidade; 3.1.56.1.6.

Consumo de memória; 3.1.56.1.7.

Disponibilidade.

3.1.56.2. Servidores Físicos: VMWARE Infraestrutura:

Datastores/FileIT:3.1.56.2.1. Espaço em Disco;

3.1.56.2.2. Consumo de

memória;3.1.56.2.3. Consumo

de discos;

3.1.56.2.4. Consumo de

processador;3.1.56.2.5. Espaço

livre de discos; 3.1.56.2.6.

Disponibilidade; 3.1.56.2.7. Taxas

de crescimento;

3.1.56.2.8. Capacidade e distribuição de

hosts;3.1.56.2.9. VMs em snapshot;

3.1.56.3. Storages:

3.1.56.3.1. Consumo de processador;

3.1.56.3.2. Utilização das

controladoras; 3.1.56.3.3. Utilização e

saúde dos discos;3.1.56.3.4.

Disponibilidade;

3.1.56.4. Integração com solução de ITSM para abertura de tickets automática e encerramentoautomático;

3.1.56.5. Servidores virtualizados e não virtualizados - Gestão de Falhas, Desempenho e Mudança:3.1.56.5.1. VMware vCenter 1 para Servidores e VMWare VCenter 3 para Desktops;

3.1.56.5.2. Active Directory R2-2012;

3.1.56.5.3. Status dos serviços;

3.1.56.5.4. DNS Server e DHCP Server;3.1.56.5.5. DFS Replication;

3.1.56.5.6. Kerberos Key Distribution Center;3.1.56.5.7. Windows Time;

3.1.56.5.8. DNS Client;

3.1.56.5.9. Security Accounts Manager;3.1.56.5.10. Server;

3.1.56.5.11. Workstation;

3.1.56.5.12. Remote Procedure Call;3.1.56.5.13. Net Logon;

3.1.56.5.14. Active Directory Domain Services;3.1.56.5.15. Contadores de LDAP;

3.1.56.5.16. Sessão em uso;

3.1.56.5.17. Tempo de pesquisa LDAP;

3.1.56.5.18. Quantidade de pesquisa por tempo;3.1.56.5.19. Bloqueio de conta

3.1.56.6. Monitoração de arquivos:

3.1.56.6.1. Alteração do conteúdo do arquivo;

3.1.56.6.2. Quantidade de arquivos em uma pasta; 3.1.56.6.3. Existência de um arquivo ou

pasta; 3.1.56.6.4. Tamanho do arquivo e tamanho

da pasta;3.1.56.6.5. Análise de arquivos de LOG;

3.1.56.6.6. Localizar uma determinada String dentro de um arquivo de LOG;

3.1.56.7. Aplicação de Atualização do Windows e/ou aplicação instalada:

3.1.56.7.1. Indicar última vez que foi instalado uma atualização Windows;

e/ou3.1.56.7.2. aplicação e se houve reinicialização do servidor;

3.1.56.8. Event Viewer:

3.1.56.8.1. Indicar um alerta/falha de

aplicação;3.1.56.8.2. Indicar logon e logout;

3.1.56.8.3. Indicar shutdown e restart com qual usuário;

3.1.56.9. Análise de Performance de Rede de Dados:

3.1.56.9.1. Deverá suportar banco de dados relacional para permitir a extração dos dados por ferramentas de terceiros;

3.1.56.9.2. Deverá permitir expansões futuras ao software adquirido acrescentando maior capacidade de dispositivos a serem monitorados;

3.1.56.9.3. A solução não deverá depender para a execução das funções descritas neste documento da instalação de agentes nos ativos monitorados;

3.1.56.9.4. Deverá possuir arquitetura para escalar a solução para quantidades maiores do que previstas neste documento, sendo possível balancear a carga da monitoração em diferentes sondas ou elementos, mantendo a administração única e sem custos adicionais além das licenças adicionais;

3.1.56.9.5. Deverá suportar nativamente a análise das comunicações IPv4 e IPv6 através da coleta de dados dos ativos de rede nos formatos NetFlow e sFlow compatíveis com os ativos de rede da CONTRATANTE;

3.1.56.9.6. A licença contratada para o quantitativo descrito neste documento deverá suportar o usode “flows” para todos os ativos existentes na infraestrutura da CONTRATANTE;

3.1.56.10. Infraestrutura – requisitos gerais:

3.1.56.10.1. Deverá suportar nativamente a coleta de dados com o uso dos protocolos SNMPv2 eSNMPv3. (get e trap), WMI, ICMP e agentes proprietários;

3.1.56.10.2. Deverá permitir de forma nativa receber traps SNMP e tratá-las através da execução de ações pela solução;

3.1.56.10.3. A solução deve ser capaz de importar e monitorar MIBs de SNMP proprietárias;

3.1.56.10.4. Deverá possuir a capacidade para autodescobrimento da rede, sendo fornecidos apenas os endereços das sub-redes e comunidade SNMP;

3.1.56.10.5. A solução deverá montar de forma automática uma topologia visual dos elementos de conectividade descobertos e inventariados, apresentando os ativos de rede com suas respectivas conexões, utilizando os protocolos LLDP ou CDP;

3.1.56.10.6. A solução deverá permitir identificar os protocolos citados a partir da análise das comunicações de qualquer ativo de rede monitorado;

3.1.56.10.7. Deverá emitir alertas e possibilitar nativamente a execução de rotinas automáticas em caso de mudanças do cenário normal. As ações possíveis devem permitir a reinicialização de serviços, executar programas externos ou comandos em CLI (Command Line Interface) diretamente no sistema operacional hospedeiro da solução;

3.1.56.10.8. Deve permitir que os dados estatísticos gerados sejam exportados em formatos HTML, PDF e CSV contendo imagens e análises da ferramenta para auxílio a resolução de problema;

3.1.56.10.9. Permitir a inserção de comentários e/ou textos descritivos em elementos monitorados;

3.1.56.11. Infraestrutura – Agentes:

3.1.56.11.1. Possuir coleta de métricas, livre de instalação de agentes, fazendo uso de SNMP, WMIe outros protocolos;

3.1.56.11.2. Possibilitar a execução de scripts nas máquinas monitoradas, sem o uso de agentes, fazendo uso de protocolos como SSH e Telnet;

3.1.56.11.3. Permitir que agentes, se usados, operem em forma passiva (o controlador inicia a comunicação) e ativa (realiza a comunicação em intervalo de tempo determinado, independente do controlador);

3.1.56.11.4. Usar criptografia na comunicação entre agentes e o controlador;

3.1.56.12. Infraestrutura - Gestão de Falhas e Desempenho de Rede:

3.1.56.12.1. Monitorar e analisar em tempo real, em profundidade, as estatísticas de desempenhode rede para quaisquer dispositivos habilitados para SNMP nas versões v1, v2 e v3, WMI e SSH;

3.1.56.12.2. Efetuar inventário dos ativos de rede indicando a conectividade entre os dispositivos, ou seja, deve ser capaz de listar qual dispositivo está conectado em cada uma de suas portas, permitindo traçar mapas de rede, sendo que estes mapas poderão ser customizados pelo usuário;

3.1.56.12.3. Deve possuir no mínimo as seguintes informações:

3.1.56.12.3.1. Nome do

dispositivo;3.1.56.12.3.2.

Endereço IP;

3.1.56.12.3.3. Nome da porta;

3.1.56.12.3.4. Dispositivo conectado;

3.1.56.13. A ferramenta deve efetuar inventário dos switches e roteadores da rede indicando:

3.1.56.13.1. O número total de portas e o status de utilização de cada uma delas;

3.1.56.13.2. Status de utilização de vLans, indicando quais switches, roteadores e quais portasfazem parte de determinada vLan;

3.1.56.13.3. vLans configuradas, incluindo seus switches e

roteadores;3.1.56.13.4. Quais dispositivos fazem parte de

determinada sub-rede;

3.1.56.14. O inventário deve conter no mínimo as seguintes informações através de coletas automáticas:
3.1.56.14.1. Categoria;
3.1.56.14.2. Descrição;

3.1.56.14.3. Tipo de dispositivo;

3.1.56.14.4. Versão do

firmware; 3.1.56.14.5. Versão

do hardware;3.1.56.14.6.

Endereço IP;

3.1.56.14.7. Localização;

3.1.56.14.8. MAC Address;

3.1.56.14.9. Modelo;

3.1.56.14.10. SNMP OID;
3.1.56.14.11. Número de

série;3.1.56.14.12. Service

Tag;

3.1.56.14.13. Fabricante;

3.1.56.14.14. Informações de garantia do

equipamento;3.1.56.14.15. EOS;

3.1.56.15. Fornecer dados históricos para fins de planejamento de capacidade, com armazenamento por período mínimo de um ano;

3.1.56.16. Fornecer informações sobre interrupções ou inoperâncias por meio de cores e/ou formato de ícones, informando se os elementos estão ou não ativos, e se os parâmetros estão ou não dentro dos limites preestabelecidos pelo fabricante;

3.1.56.17. Realizar descobrimento automático da topologia de nível 2 e nível 3 da rede para apresentação do mapa de conectividade e de informações de configurações dos elementos;

3.1.56.17.1. O descobrimento de nível 2 deverá suportar pelo menos os seguintes métodos depesquisa:

3.1.56.17.1.1. Consulta a tabelas ARP;

3.1.56.17.1.2. Consulta a tabelas de endereços

IP;3.1.56.17.1.3. Consulta a tabelas de

roteamento

3.1.56.17.1.4. Consulta a informações de Spanning Tree.

3.1.56.18. Acompanhar o desempenho dos links contratados e VPN em tempo real; via Probe devido à falta de acesso SNMP nos routers das operadoras e via interface do dispositivo de rede interno;

3.1.56.19. Permitir a criação de grupos de dispositivos, interfaces ou grupos parametrizáveis e análise de disponibilidade deles;

3.1.56.20. Permitir a correlação de eventos através da criação de dependências entre grupos parametrizáveis e dispositivos de rede;

3.1.56.21. Habilitar alertas para eventos correlacionados, condições mantidas e combinações

complexas de estados de dispositivos. Devendo incluir no mínimo:

3.1.56.21.1. Causa da falha;

3.1.56.21.2. Severidade;

3.1.56.21.3. Hora de início e

fim;

3.1.56.21.4. Descrição do

dispositivo;3.1.56.21.5. Endereço

IP.

3.1.56.22. As notificações devem suportar no mínimo os seguintes

formatos:3.1.56.22.1. E-mail;

3.1.56.22.2. SNMP Traps;

3.1.56.23. As notificações devem permitir no mínimo a execução das seguintes

ações:3.1.56.23.1. Execução de aplicações externas;

3.1.56.23.2. Mensagens de Syslog;

3.1.56.23.3. Execução de scripts;

3.1.56.23.4. Start e restart de

serviços;

3.1.56.24. Permitir a categorização dos ativos de rede por geolocalização, ou departamento, assimcomo a criação de novas categorias para a classificação deles.

3.1.56.25. Permitir acréscimo de monitoramentos personalizados através da inclusão de MIB's nosistema.

3.1.56.26. Conter mecanismos ou ferramentas inclusas de MIB Walker, MIB Explorer e Gerenciadorde MIB's SNMP.

3.1.56.27. Possuir um centro de mensagens único para todos os alertas de eventos em dispositivos e/ou serviços de maneira a permitir correlação desses eventos.

3.1.56.28. Permitir a configuração ou agendamento de descobrimento automático na rede.

3.1.56.29. Permitir a criação de relatórios de rede personalizados, que possam ser impressos ou visualizados na interface web, e exportados para os formatos PDF e planilhas eletrônicas compatíveis com o Microsoft Office 365 e superiores;

3.1.56.30. Permitir adição de mapas gráficos escolhendo entre vários modelos integrados geograficamente ou importar imagem lógica da rede.

3.1.56.31. Deve possibilitar a consulta de tabela das interfaces de rede, incluindo nome, velocidade, status, tráfego de entrada e saída e erros de entrada e saída, assim como descartes de pacotesnas interfaces;

3.1.56.32. Deve possibilitar a consulta de informações da tabela ARP, tanto IPV4 quanto IPV6.

3.1.56.33. Deve possibilitar a consulta da tabela de roteamento, tanto IPV4, quanto IPV6.

3.1.56.34. Deve possibilitar consultas as informações de desempenho do sistema gerenciado, incluindo:

3.1.56.34.1. Utilização de partições de disco, em valor absoluto e percentual;

3.1.56.34.2. Estatísticas dos discos físicos (input e output), incluindo quantidade de leituras e escritas;

3.1.56.34.3. Tabela de processos incluindo ID do processo, memória usada, tamanho, tempo deCPU, horário de início, processo pai e número de threads;

3.1.56.34.4. Tabela dos principais processos do sistema.

3.1.56.34.5. Ferramenta deve ser capaz de executar análise em tempo real possibilitando:

3.1.56.34.5.1. Selecionar um grupo de dispositivos e consultar uma variável do dispositivo a intervalos regulares de tempo e colocar os valores em gráficos;

3.1.56.34.5.2. Selecionar um grupo de variáveis de um dispositivo e consultar o seu valor a intervalos regulares de tempo e colocar esses valores em gráficos;

3.1.56.34.5.3. Incluir os valores em um único gráfico ou em vários gráficos;

3.1.56.34.5.4. Obter informação histórica pelo menos 1 hora antes de iniciar a análise em temporeal;

3.1.56.34.5.5. Gravar estes perfis de análise em tempo real para o seu uso posterior.

3.1.56.35. Linux:

3.1.56.35.1. CPU Usado, em Idle;

3.1.56.35.2. CPU em espera de I/O;

3.1.56.35.3. Fila de processos para

execução;3.1.56.35.4. Interrupção por

segundo;

3.1.56.35.5. Disco – Tempo de leitura de

cache;3.1.56.35.6. Espaço por partição;

3.1.56.35.7. Leitura e escrita de blocos por

segundo;3.1.56.35.8. Memória RAM Total;

3.1.56.35.9. Memória RAM usada;3.1.56.35.10. Uso de SWAP;

3.1.56.35.11. Espaço total de SWAP;3.1.56.35.12. Processos Zumbi;

3.1.56.35.13. Número de processos com um determinado nome;

3.1.56.36. Windows Server 2003, 2008, 2012 incluindo o R2, 2016, 2019 e superior:3.1.56.36.1. Status dos serviços;

3.1.56.36.2. Distributed Transaction Coordinator;3.1.56.36.3. Security Accounts Manager; 3.1.56.36.4. Remote Registry;

3.1.56.36.5. Plug and Play;

3.1.56.36.6. Total de memória disponível;3.1.56.36.7. % de memória em uso;

3.1.56.36.8. Tamanho do arquivo de SWAP usado;3.1.56.36.9. Uso em % dos processadores;

3.1.56.36.10. Número de páginas escritas ou lidas do disco por segundo;

3.1.56.36.11. Tamanho da fila de requisições para acesso ao disco físico e logico;3.1.56.36.12. Monitorar Windows Event Log Monitor;

3.1.56.36.13. Espaço nas partições;

3.1.56.36.14. Número de processos com um determinado nome;

3.1.56.36.15. Impacto no host físico, se Windows for virtual, objetivo identificar se existe problemade performance no device físico;

3.1.56.36.16. Quem e quando fez último logon e logoff;

3.1.56.37. Windows Domain Controllers 2012 (Controladores de domínio):3.1.56.37.1. Número de usuários bloqueados e desabilitados;

3.1.56.37.2. Alerta de usuário bloqueado;

3.1.56.37.3. Número de novas contas criadas;

3.1.56.37.4. Número de tentativas logons de um usuário (ataque de força bruta);

3.1.56.37.5. Alerta de tentativa de logon e falha por senha ou compatibilidade Kerberos;3.1.56.37.6. Número de contas ativas sem uso por mais de 30 dias;

3.1.56.37.7. Número de alterações na política Kerberos do domínio;

3.1.56.37.8. Alerta de falha Kerberos;

3.1.56.37.9. Número de alterações na política de auditoria do domínio;
3.1.56.37.10. Número de desligamento do servidor;

3.1.56.37.11. Número de alterações na hora do sistema;

3.1.56.37.12. Windows Update (rotina executada pelo Qualys Patch management);3.1.56.37.13. Número de dias desde a última atualização;

3.1.56.37.14. Alerta de servidor precisando reiniciar para aplicar atualização;3.1.56.37.15. Alerta indicando se o servidor está instalando atualizações;

3.1.56.38. Windows DHCP Server:

3.1.56.38.1. Número de Pacotes recebido por segundo; 3.1.56.38.2. Número de pacotes duplicados descartados;3.1.56.38.3. Tamanho da fila ativa;

3.1.56.38.4. Requisições por segundo;

3.1.56.38.5. Acks e Nacks por segundo;

3.1.56.38.6. Release (Renovação de ip) por segundo;

3.1.56.38.7. Status do serviço: DHCP Server;

3.1.56.38.8. Alertas em caso de erro no Jet Database;

3.1.56.38.9. Alerta em caso de esgotamento de IP livres em um escopo;

3.1.56.39. Windows DHCP Server:

3.1.56.39.1. Uso de memória do banco de dados do DNS;

3.1.56.39.2. Número de atualizações dinâmicas recebidas e rejeitadas;3.1.56.39.3. Número de Consultas recursivas por segundo; 3.1.56.39.4. Número de Consultas recursivas que falhou por segundo;

3.1.56.39.5. Número de Consultas recursivas que falou por timeout por segundo;3.1.56.39.6. Status do serviço: DNS Server;

3.1.56.39.7. Número de Consultas recebidas por segundo em TCP e UDP; 3.1.56.39.8. Número de Consultas respondidas por segundo em TCP e UDP;

3.1.56.40. Windows Servidores de

Impressão:3.1.56.40.1. Número de Jobs
com erro; 3.1.56.40.2. Número de Jobs no
spool; 3.1.56.40.3. Número de Jobs;

3.1.56.40.4. Monitor do serviço: Print Server
Spooler;3.1.56.40.5. Número de Threads do Print
Server;

3.1.56.41. Windows Remote Desktop Services Licensing:

3.1.56.41.1. Número de licenças em uso

3.1.56.41.2. Monitora o serviço: Remote Desktop Licensing

3.1.56.41.3. Erros de inicialização no Event sobre serviço de
licenciamento.3.1.56.41.4. Erros de Database no Event sobre serviço
de licenciamento.
3.1.56.42. SSL Certificado em servidor WWW
3.1.56.42.1. Verifica se o servidor aceita conexões
SSL.3.1.56.42.2. Verifica a data de expiração do
certificado.
3.1.56.43. Internet Information Services (IIS)

3.1.56.43.1. Serviço WEB: Contador de Bytes Recebidos por
tempo3.1.56.43.2. Serviço WEB: Contador de Bytes enviados
por tempo 3.1.56.43.3. Serviço WEB: Contador de conexões
ativa
3.1.56.43.4. Serviço WEB: Contador de GET por tempo

3.1.56.43.5. Monitor de status do serviço: World Wide Web Publishing

3.1.56.43.6. Testa um formulário básico de autenticação como um

usuário.

3.1.56.44. Servidor HTTP

3.1.56.44.1. Monitorar a disponibilidade e tempo de resposta de um servidor externo à infraestruturada Copel Telecom, em HTTP e HTTPS

3.1.56.45. Oracle Database

3.1.56.45.1. Espaço livre em

%

3.1.56.45.2. Espaço usado na Tablespace em %

3.1.56.45.3. Relação de uso do cache de dicionário em relação aos pedidos

totais3.1.56.45.4. Número de usuários conectados

3.1.56.45.5. Tamanho dos arquivos temporários

3.1.56.45.6. Tamanho dos arquivos de dados (Data

Files)

3.1.56.45.7. Número de operações de sort que foram executadas completamente na memória

3.1.56.45.8. Número de rollbacks manuais por usuários

3.1.56.46. Citrix Presentation Server e Citrix Metaframe

Server3.1.56.46.1. Citrix IMA Networking: Conexões de

rede

3.1.56.46.2. Citrix Licensing: Tempo de resposta (ms) do servidor de

licença3.1.56.46.3. Citrix Licensing: Licença Falha de conexão do

servidor

3.1.56.46.4. Citrix sessão ICA: Latency – Last Recorded

3.1.56.46.5. Citrix sessão ICA: Latency – Session Average

3.1.56.46.6. Citrix sessão ICA: Latency – Session Deviation

3.1.56.46.7. Citrix Presentation Server: Número de threads ocupado

XML 3.1.56.46.8. Citrix Presentation Server: Número de sessões ativas

3.1.56.46.9. Citrix Presentation Server: Número de sessões

desconectadas3.1.56.46.10. Monitora pelo menos os serviços:

3.1.56.46.11. Citrix Services Manager; Citrix Print Manager Service; Citrix WMI Service; Citrix Licensing (no servitor de Licença);

3.1.56.46.12. Citrix Group Policy Engine e Citrix Licensing Support Service, Citrix MFCOM Service(Metaframe COM Server), Citrix Independent Management Architecture

3.1.56.47. Lotus Domino Server

3.1.56.47.1. Uso de memória e CPU do processo Administrative

Process3.1.56.47.2. Uso de memória e CPU do processo Agent

Manager 3.1.56.47.3. Uso de memória e CPU do processo Calendar

Connector 3.1.56.47.4. Uso de memória e CPU do processo Event

Monitor 3.1.56.47.5. Uso de memória e CPU do processo IMAP

Server 3.1.56.47.6. Uso de memória e CPU do processo LDAP

Server 3.1.56.47.7. Uso de memória e CPU do processo POP3

Server 3.1.56.47.8. Uso de memória e CPU do processo Replicator

3.1.56.47.9. Uso de memória e CPU do processo Router

3.1.56.47.10. Uso de memória e CPU do processo Schedule

Manager3.1.56.47.11. Uso de memória e CPU do processo

Database Server 3.1.56.47.12. Uso de memória e CPU do

processo Indexer 3.1.56.47.13. Números de sessões abertas

3.1.56.47.14. Recursos disponíveis em %

3.1.56.47.15. Número de Task LDAP

3.1.56.48. Tomcat Server (JMX)

3.1.56.48.1. Memória livre da heap na

JVM

3.1.56.48.2. Memória ocupada da heap na JVM

3.1.56.48.3. Memória máxima da heap na JVM

3.1.56.48.4. Tempo total de processamento do ervidor

3.1.56.48.5. Total de Bytes recebido e enviados

3.1.56.48.6. Número de requisições

3.1.56.48.7. Número de erros requisições de processamento

3.1.56.49. VMware ESX Host

3.1.56.49.1. Usando a API do VMware fornece as seguintes

métricas:3.1.56.49.2. CPU Reserved Capacity. Average

3.1.56.49.3. CPU Usage (Average). average

3.1.56.49.4. CPU Usage in MHz (Average).

average 3.1.56.49.5. Disk Usage (Average).

average 3.1.56.49.6. Memory Active (Average).

average 3.1.56.49.7. Memory Balloon (Average).

average 3.1.56.49.8. Memory Consumed

(Average). average 3.1.56.49.9. Memory Granted

(Average). average 3.1.56.49.10. Memory Heap

(Average). average 3.1.56.49.11. Memory Heap

Free (Average). average3.1.56.49.12. Memory

Overhead (Average). average 3.1.56.49.13.

Memory Reserved Capacity. Average

3.1.56.49.14. Memory Shared (Average). average

3.1.56.49.15. Memory Shared Common (Average).

average3.1.56.49.16. Memory State. Latest

3.1.56.49.17. Memory Swap In (Average). average

3.1.56.49.18. Memory Swap Out (Average).

average 3.1.56.49.19. Memory Swap Used

(Average). average3.1.56.49.20. Memory

Unreserved (Average). average3.1.56.49.21.

Memory Usage (Average). average 3.1.56.49.22.

Memory Used by vmkernel. average 3.1.56.49.23.

Memory Zero (Average). average 3.1.56.49.24.

Network Usage (Average). average 3.1.56.49.25.

System.Uptime. latest

3.1.56.50. VMware vCenter Server

3.1.56.50.1. Uso de CPU e memoria só serviço: VMWare Certificate

3.1.56.50.2. Uso de CPU e memoria só serviço: VMware

Directory3.1.56.50.3. Uso de CPU e memoria só serviço:

VMware Kdc

3.1.56.50.4. Uso de CPU e memoria só serviço: VMware vCenter Inventory

3.1.56.50.5. Uso de CPU e memoria só serviço: VMware Virtual Center Management

Webservices3.1.56.50.6. Uso de CPU e memoria só serviço: VMware Virtual Center Server

3.1.56.50.7. Uso de CPU e memoria só serviço: VMware vSphere Web Client

3.1.56.50.8. Testar se o VCenter está pronto para receber conexão nas portas HTTP, HTTPS,LDAP, SSL

3.1.56.51. Infraestrutura – robôs de testes sintéticos

3.1.56.51.1. Monitor que simula o uso de um cliente de DNS onde se mede o

tempo de3.1.56.51.2. resposta do servidor DNS e se as respostas são os

endereços esperados

3.1.56.51.3. Monitor que simula que realiza consulta em bancos de dados usando driver ODBCreportando as métricas de tempo para recebimento dos dados criando

3.1.56.51.4. base estatística para análise de performance.

3.1.56.51.5. Monitor que simula que realiza consulta em bancos de dados ORACLE não fazendouso de driver ODBC reportando as métricas de tempo para recebimento dos dados criando base estatística para análise de performance.

3.1.56.51.6. Monitor que simula que realiza conexões com servidor FTP realizando autenticação de usuário e download de um arquivo, identificando tempo de download e teste de integridade deste arquivo.

3.1.56.51.7. Monitor que simule o acesso a uma página web HTTP:

3.1.56.51.8. Identifique a quantidade de bytes recebidos

3.1.56.51.9. Pesquise uma String para verificação do

conteúdo3.1.56.51.10. Retorne o tempo de acesso

3.1.56.52. Monitoramento IBM MQ

3.1.56.53. Monitoramento de Storage Dell

3.1.56.53.1. Monitoramento de Storage Dell

XtremIO

ITEM 10 –SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO

3.1.57. A implantação da solução deve seguir as boas práticas de mercado no

gerenciamento de projetos, bem como as boas práticas e diretrizes do FABRICANTE da solução.

3.1.58. Deverão observar integralmente os requisitos de projeto da solução de segurança e deimplementação descritos a seguir:

▪ O cálculo de horas para suporte on-site de cada solução prevista, instalação e configuração das licenças dos softwares de segurança é de 15% (quinze por cento) da quantidade de licenças que serão contratadas, podendo ser adequada pela unidade CONTRATANTE (maior ou menor) de acordo com a necessidade.

▪ A CONTRATANTE, no momento da assinatura do contrato, deverá apresentar a certificação dos técnicos mediante certificados emitidos pelo fabricante da solução de segurança.

▪ Instalação e configuração total de todas as licenças do software de segurança adquirido no ambiente físico/virtual da CONTRATANTE, no prazo máximo de 45 (quarenta e cinco) dias após a emissão da ordem de serviço;

▪ É de responsabilidade da CONTRATADA a remoção remota da solução antiga de solução de segurança, atualmente instalada nos equipamentos da CONTRATANTE. O projeto de implementação das licenças dos softwares de segurança deverá ser conduzido em etapas:

▪ **Iniciação:** a CONTRATADA deverá criar a visão do projeto e definirá o escopo de trabalho

necessário para trazê-la para a realidade;

▪ **Planejamento**: deverá consistir na elaboração de um Plano Técnico a serem utilizados na

implantação do projeto;

▪ **Implementação**: consistirá na execução das atividades definidas na fase de planejamento,

podendo ser dividida em sub-bases para melhor controle;

▪**Estabilização**: a solução deverá ser disponibilizada para os usuários do ambiente de produção, sendo efetuados os ajustes necessários para a estabilização dela;

▪ **Encerramento:** Deverá ser entregue a documentação do projeto, e coletada a aprovação formal do cliente;

3.1.59. Da inicialização e planejamento:

▪ Reunião de startup;
▪ Apresentação dos requisitos necessários de infraestrutura para início do projeto;
▪ Definição e alinhamento de cronograma para implementação das soluções;
▪ Levantamento de informações do ambiente pertinentes ao projeto de implementação;
▪ Alinhamento de requisitos necessários para implementação das soluções;
▪ Levantamento de políticas e regras para planejamento, implementação e configurações solução de segurança;
▪ Definição de papéis e responsabilidades;
▪ O prazo para entrega da CONTRATADA do planejamento de implementação das soluções de segurança devem ser de no máximo 15 (quinze) dias da assinatura do contrato e a CONTRATANTE tem 5 (cinco) dias para dar o aceite no projeto;
▪ A partir da data de aceite, por parte da CONTRATANTE, ao projeto e cronograma entregues pela CONTRATADA. Esse prazo é referente às atividades da CONTRATADA. Não estarão aí contabilizadas as atividades de responsabilidade da CONTRATANTE;

▪ A CONTRATADA deverá apresentar um projeto para desinstalação remota da solução de segurança existente em toda a rede da CONTRATANTE.
▪ Não serão considerados responsabilidade da CONTRATADA implementação de agentes em equipamentos fora de pré-requisitos estabelecidos pelo fabricante e sem conectividade com a console central de administração da solução.

3.1.60. Da implementação da solução de segurança:

- Deverão acompanhar 30% de implementação nas dependências da CONTRATANTE em conjunto com a equipe de analistas de segurança da informação da CONTRATADA ou conforme acordado com a CONTRATANTE;

- O serviço de implementação preferencialmente será realizado nas dependências da CONTRATANTE, em horário comercial, das 08h00 às 18h00, de segunda a sexta-feira, excetuando-se feriados nacionais e estaduais ou conforme acordado com a CONTRATANTE. Quando se tratar de equipamentos críticos (servidores, storages, dispositivos móveis, entre outros), estas implementações poderão ser realizadas fora dehorário comercial e/ou nos finais de semana.

- Instalação e configurações globais das consoles de administração da solução de
- segurança.Integração de todos os itens que compõem a solução de modo a permitir a visão e o gerenciamento em uma única console;

- Deverá ser utilizada como método de instalação (deploy) dos agentes nos equipamentos daCONTRATANTE, a instalação remota via console da solução contratada ou solução de distribuição similar sem custos adicionais. A CONTRATANTE fornecerá os pré-requisitos para viabilidade da instalação remota via console da solução;

- Instalação (deploy) dos agentes da solução em servidores físicos e virtuais, incluindo remoção remota dos agentes existentes quando aplicável;

- Instalação (deploy) dos agentes da solução em desktops e notebooks, que fazem ou não parte do domínio local (Active Directory), incluindo remoção remota dos agentes existentesquando aplicável, desde que possuam comunicação de rede com a rede principal da CONTRATANTE;

- Geração de pacotes de instalação (deploy), para a equipe da CONTRATANTE realizar a instalação da solução de segurança nos equipamentos que não possuem comunicação derede com a rede principal da CONTRATANTE, incluindo remoção remota dos agentes existentes quando aplicável;

- Durante a fase de implementação a CONTRATADA deverá disponibilizar técnicos capacitados para acompanhamento em cada uma das equipes de implantação, com objetivode resolver problemas de acesso físico e logico às localidades;

- À CONTRATADA ficará a cargo de efetuar a remoção remota prévia dos agentes em servidores devido a criticidade do ambiente;

- Criação de políticas de segurança em conjunto com as equipes técnicas da CONTRATANTE.

3.1.61. Do encerramento:

- Será considerada concluída a implementação da solução de segurança quando o número de equipamentos protegidos for igual ou superior a 60% do volume de equipamentos existentes.

3.1.62. Da estabilização:

- Deverão executar Health Check (saúde das consoles) nas soluções de segurança semestralmente, englobando:

    - Validar as configurações do servidor da console de gerenciamento da solução de segurança;

    - Validar as políticas da solução de segurança;

- Revisar a configuração da infraestrutura da solução de segurança; o Criar um relatórioque sugira melhorias com base nas melhores práticas da solução de segurança;

ITEM 11 – TREINAMENTOS DOS SOFTWARES LICENCIADOS

- Cada módulo de treinamento deverá ser de no mínimo 16 horas de duração.
- O treinamento deve ser realizado de segunda a sexta-feira (dias úteis), entre 8h (oito) horase 18h (dezoito) horas.
- Para cada módulo da solução contratada, o treinamento oficial deverá ser efetuado pelofabricante ou entidade credenciada com a emissão de certificados individuais para os colaboradores;
- Os treinamentos consistirão na capacitação de técnicos dos órgãos participantes do SRP nosprocessos de trabalho, métodos, técnicas e ferramentas integrantes da solução de segurançaimplantada;
- O mesmo deverá ser realizado, dentro da região de São Paulo ou remotamente, a critério daCONTRATANTE;
- Deverá ser emitido um certificado para cada participante do
- treinamento;Aceite por parte da CONTRATANTE.

Requisitos de Manutenção

- Devido às características da solução de segurança, há necessidade de realização de manutenções corretivas e evolutivas da solução de segurança pela CONTRATADA e pelo fabricante da solução de segurança, visando à manutenção da disponibilidade da
- solução; Os softwares da solução de segurança terão suas atualizações pelo prazo de validade de 36(trinta e seis) meses.
- O serviço de suporte técnico da solução de segurança deverá ser de 36 (trinta e seis) mesesprestado pelo fabricante em regime 24 x 7 x 365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) contra falhas e correções, disponibilizando as atualizações de versão e definição de vírus periodicamente.
- A CONTRATADA deverá fornecer e-mail, número telefônico e/ou opção via website paraabertura de chamados técnicos, estes deverão possuir identificador (numérico) próprio, repassado ao CONTRATANTE, a fim de registro e acompanhamento das ocorrências.

- O suporte técnico prestado pela CONTRATADA consiste no esclarecimento de dúvidas, nareparação das eventuais falhas de funcionamento, mediante a substituição de versão, de acordo com os manuais e normas técnicas específicas do produto, bem como, orientação das melhores práticas de uso dos produtos adquiridos.

- Entende-se por término do atendimento, das ocorrências em aberto, a disponibilidade parauso em perfeitas condições de funcionamento no local onde está instalado, estando condicionado à aprovação do CONTRATANTE.

- Para a solução de segurança, uma vez registrada a ocorrência junto à CONTRATADA, elaserá encaminhada para os procedimentos de atendimento e solução dos problemas, devendo ter como objetivos de atendimento os índices de criticidade determinados pelo FABRICANTE, descritos a seguir:

Criticidade	**Descrição**	**Atendimento**	**Resolução do Atendimento**
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema, ou dos dados. Exemplo: Serviço inativo.	30 minutos a 1 hora	Menos de 4horas
Severidade2 (Média /Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade. a curto prazo, possa ser afetada negativamente. Exemplo: Servidor não responde a comandos ou responde com resultados inesperados. Arquivos de *log* corrompidos ou inexistentes.	4 a 6 horas	Menos de 10horas

Severidade3 (Baixa)	Demais problemas que não afetem diretamente o ambiente de produção. Exemplo: Problemas na geração de relatórios e dúvidas gerais de operação/configuração.	8 a 10 horas	Menos de 30horas

Além do atendimento nos níveis de criticidade citados no subitem anterior, a CONTRATANTE terá o direito de, no mínimo, 2 (duas) visitas técnicas anuais presenciais ou conforme acordado com a CONTRATANTE, para realização de serviçotécnico de *CyberSecurity Health Check* com análise e validação de processos administrativos de segurança da infraestrutura dos softwares de segurança da CONTRATANTE de acordo com as melhores práticas do fabricante, realizadas por técnicos certificados e especialistas.

4. Requisitos da contratação

5. REQUISITOS DA CONTRATAÇÃO
5.1. A descrição da solução como um todo encontra-se pormenorizada em tópico 3 deste Termo deReferência,

Indicação de marcas ou modelos (*Art. 41, inciso I, da Lei nº 14.133, de 2021*):

5.2. Na presente contratação será admitida a indicação da(s) seguinte(s) marca(s), característica(s)ou modelo(s), de acordo com as justificativas contidas nos Estudos Técnicos Preliminares.

5.3. Da exigência de carta de solidariedade

Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelofabricante, que assegure a execução do contrato.

5.3.1. Declaração, específica para este certame, emitida pelo fabricante, comprovando que o licitante está apto e qualificado a vender e comercializar as soluções e os serviços técnicos objeto deste Termo de Referência. Se a equipe técnica da CONTRATANTE achar necessário, ele poderá realizar diligência para confirmar a veracidade das informações fornecidas;

5.3.1.1. A declaração específica solicitada acima deverá ser apresentada em papel timbrado, original ou cópia reprográfica autenticada, assinado(s) por autoridade ou representante de quem o

(s) expediu, com a devida identificação;

5.3.2. A proponente deverá comprovar para os itens de 01 à 06, por meio de declaração formal emitida pelo fabricante da solução de segurança que é uma revenda autorizada com classificação “GOLD PARTNER” ou “PLATINUM PARTNER”, e que está apta a comercializar e prestar assistência e suporte "on-site" para a solução proposta.

5.3.2.1. A exigência do credenciamento se justifica em razão de que o fornecedor deverá possuir todo o suporte técnico direto com o fabricante do software, evitando possível ausência no fornecimento de suporte ou de atualizações e um quadro de profissionais certificados, visando uma prestação dos serviços de excelência à esta municipalidade;

5.3.2.2. A exigência do credenciamento com a referida classificação se baseia, dentre outros, na relevância da prestação do serviço, que trata de segurança cibernética, que enseja a prestação de serviço por empresas altamente especializadas capazes de atender demandas de urgência com a devida e necessária efetividade, que é a capacidade de realizar uma demanda (eficácia) da melhor maneira possível (eficiência).

5.4. Subcontratação

5.4.1. Não é admitida a subcontratação do objeto contratual.

5.4.2. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidosna licitação original, sejam mantidas as demais cláusulas e condições contratuais, não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidadecontratual.

5.5. Garantia da Contratação

5.5.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.

5.5.2. No prazo de convocação para formalização da contratação, e anteriormente à celebração da contratação, o fornecedor deverá prestar garantia, podendo optar por uma das seguintes modalidades:

I - **Caução em dinheiro**. A garantia em dinheiro deverá ser efetuada mediante depósito

bancário em favor do Contratante no Banco do Brasil, em conta que contemple a correção monetária do valor depositado.

II - **Caução em títulos da dívida públic**a. Serão admitidos apenas títulos da dívida pública

emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério competente.

III - **Fiança bancária**. Feita a opção pela fiança bancária, no instrumento deverá constar a

renúncia expressa do fiador aos benefícios do artigo 827 do Código Civil. Será admitida fiança bancária emitida por banco ou instituição financeira devidamente autorizada a operar no Paíspelo Banco Central do Brasil.

IV - **Seguro-garantia**. A apólice de seguro-garantia somente será aceita se contemplar todos os

eventos indicados em conformidade com a subdivisão posterior, observada a legislação querege a matéria. Caso tal cobertura não conste expressamente da apólice, o fornecedor vencedor poderá apresentar declaração firmada pela seguradora emitente afirmando que o seguro- garantia apresentado é suficiente para a cobertura de todos os eventos indicados em conformidade com a subdivisão posterior, observada a legislação que rege a matéria.

V - **Título de capitalização**. Serão admitidos apenas títulos de capitalização conforme a

modalidade instrumento de garantia custeados por pagamento único, com resgate pelo valortotal, emitidos com observância da legislação que rege a matéria.

5.5.3. A não prestação da garantia equivale à recusa injustificada de formalização da contratação, caracterizando descumprimento total da obrigação assumida e sujeitando o fornecedor vencedor às sanções previstas nas normas pertinentes.

5.5.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

5.6. Vistoria

5.6.1. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessadoo direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sextafeira, das 09:00 horas às 16h horas.

5.6.2. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

5.6.3. Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

5.6.4. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

5.7. DA APRESENTAÇÃO DA PROPOSTA

A proposta deverá ser apresentada, com valores em real, redigida em português, em formulário oficial da empresa, que contenha a razão social, endereço, telefone, e-mail e CNPJ e nela deverão constar os requisitos a seguir especificados:

5.7.1. Será exigida ao LICITANTE, na apresentação da proposta comercial, a identificação completa dos itens de comprovação compulsória, como nome do fabricante e modelo/ part number das licenças a serem utilizados na execução dos serviços.

5.7.2. A licitante deverá junto com a entrega da proposta comercial, encaminhar toda documentação, manuais, folhetos, sites “impressos” da WEB e demais materiais de referência de forma digital que comprovem efetivamente comprove a existência e aderência ao quesito ou padrão exigido às especificações técnicas descritas nesse Termo de Referência.

5.7.3. As características técnicas obrigatórias deverão estar grifadas ou destacadas na documentação entregue, além de estarem todas relacionadas em tabela específica indicando o número da página da documentação onde encontrar sua comprovação, de forma a garantir uma rápida e melhor análise.

5.7.4. O não atendimento as características técnicas mínimas exigidas ou a comprovação de que a solução proposta possui características inferiores às solicitadas ensejará a desclassificação do participante do processo licitatório.

5.7.5. Toda a documentação exigida neste item assegura à contratante maior isonomia na avaliação técnica das propostas das empresas licitantes, além de oferecer objetivamente o entendimento correto do escopo de fornecimento da solução ofertada.

5.7.6. Os preços ora propostos incluem todas as despesas diretas, indiretas, benefícios, tributos, contribuições, seguros e licenças de modo a se constituírem em única e total contraprestação pelo fornecimento dos materiais ou serviços.

6. Modelo de execução do objeto

5.1. Condições de Entrega

5.1.1. O prazo de entrega dos bens é de 10 (dez) dias, contados do(a) recebimento da Ordem de Serviço (OS), em remessa única.

5.1.2. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 10 (dez) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

5.1.3. Os bens deverão ser entregues no endereço que será informado na OS.

5.1.4. Todos os serviços eventualmente previstos deverão ser executados em conformidade com as metodologias e padrões estabelecidos pelo CONTRATANTE. O CONTRATANTE poderá adotar novos padrões, metodologias, arquiteturas ou tecnologias durante a execução contratual, desdeque forneça prazo mínimo de 45 (quarenta e cinco) dias corridos para que a CONTRATADA possase adequar ao novo cenário adotado.

5.1.5. A CONTRATADA deverá elaborar um cronograma para atendimento, a ser aprovado pelo CONTRATANTE. A CONTRATADA deverá entregar os produtos e serviços encomendados de acordo com o cronograma e dentro dos padrões de qualidade e de compatibilidade técnica, conforme as metodologias e padrões do CONTRATANTE.

5.1.6. O CONTRATANTE poderá adotar, a seu critério, um sistema informatizado para gerenciar o encaminhamento e controle de solicitações, bem como para monitorar a execução e realizar o acompanhamento dos serviços.

5.1.7. As licenças deverão ser acompanhadas de suporte técnico, garantia e direito a atualização de versão. Ao longo de todo o contrato o CONTRATANTE poderá a qualquer

momento demandar apoio técnico através de chamados em plataforma disponibilizada pela CONTRATADA. O atendimento aos chamados de suporte técnico será prestado na modalidade remota.

5.1.8. As licenças dos softwares de segurança deverão ser instalados e configurados nos equipamentos indicados, atendendo a todos os requisitos de segurança da informação estabelecidos pelo CONTRATANTE.
5.1.9. Todos os detalhes e procedimentos de instalação e configuração da solução de segurança deverão ser documentados pela CONTRATADA e entregues ao CONTRATANTE em formato definido por este.

5.1.10. Durante os procedimentos de instalação e configuração da solução de segurança a CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica designada pelo CONTRATANTE, contemplando toda a estrutura metodológica utilizada na execução dos serviços.

5.1.11. A execução dos serviços inerentes à implantação da solução de segurança deverá ser realizada por profissionais devidamente identificados e com experiência comprovada através de certificados pelo fabricante da solução.

5.1.12. O CONTRATANTE deverá fornecer ambiente adequado para instalação das soluções e acesso aos colaboradores da CONTRATADA quando necessário.

5.2. Garantia, manutenção e assistência técnica

O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo 36 (trinta e seis) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto. Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.

6. Modelo de gestão do contrato

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.
6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.
6.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
6.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. Após a assinatura do contrato ou instrumento equivalente (caso assim definido pela documentação que compõe a presente contratação), o órgão ou entidade poderá convocar o representante da contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das

estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

Fiscalização

6.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

Fiscalização Técnica

6.7. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 68.220, de 2023, art. 17°);

6.7.1. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e 68.220, de 2023, art. 17, II);

6.7.2. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Lei federal nº 14.133, de 2021, artigo 117, § 2º)

6.7.3. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto estadual nº 68.220, de 2023, art. 17, II).

Fiscalização Administrativa

6.8. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Decreto estadual nº 68.220, de 2023, art. 18, II e III).

6.8.1. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto estadual nº 68.220, de 2023, art. 18, IV).

6.8.2. Sempre que solicitado pelo Contratante, a Contratada deverá comprovar o cumprimento da reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, com a indicação dos empregados que preencherem as referidas vagas, nos termos do parágrafo único do artigo 116 da Lei federal nº 14.133, de 2021.

6.9. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

6.9.1. Fiscalizar as atividades realizadas pela CONTRATADA, acompanhando seus indicadores de produção e qualidade;

6.9.2. Conduzir reuniões de acompanhamento e pontos de checagem quando julgar necessários para garantir o bom andamento da prestação dos serviços.

Gestor do Contrato

6.10. O gestor do contrato exercerá a atividade de coordenação dos atos de fiscalização técnica, administrativa e setorial e dos atos preparatórios à instrução processual visando, entre outros, à prorrogação, à alteração, ao reequilíbrio, ao pagamento, à eventual aplicação de sanções e à extinção dos contratos (Decreto estadual nº 68.220, de 2023, inciso III do art. 2º.

6.11. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto estadual nº 68.220, de 2023, art. 16, IX).

6.12. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto estadual nº 68.220, de2023, art. 18, VII).

6.13. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal,conforme o caso. (Decreto estadual nº 68.220, de 2023, art. 16, VIII).

6.14. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto estadual nº 68.220, de 2023, art. 16, VIIe parágrafo único).

6.15. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7. Critérios de medição e pagamento

Recebimento

7.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega,

juntamentecom a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

7.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação do Contratado, às suas custas, sem prejuízo da aplicação das penalidades.

7.3. O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

7.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até 10 (dez) dias úteis.

7.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.6. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, se houver parcela incontroversa, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, com a comunicação ao contratado para emissão de Nota Fiscal/Fatura no que pertinente à parcela incontroversa, para efeito de liquidação e pagamento.

7.7. O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

7.8. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Liquidação

7.9. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez)dias úteis para fins de liquidação, a contar de seu recebimento pela Administração, na forma desta seção, prorrogáveis por igual período, justificadamente, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais (art. 7º, I, e §§ 2º e 3º, da Instrução Normativa SEGES/ME nº 77, de 4 de novembro de 2022, c/c o Decreto estadual nº 67.608, de 2023).

7.9.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação nele especificada, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do caput do art. 75 da Lei nº 14.133, de

2021.

7.10. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como, caso aplicáveis:

7.10.1. o prazo de validade;

7.10.2. a data da emissão;

7.10.3. os dados do contrato e do órgão contratante;

7.10.4. o período respectivo de execução do contrato;o valor a pagar; e

7.10.5. eventual destaque do valor de retenções tributárias cabíveis.

7.11. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularizaçãoda situação, sem ônus ao contratante;

7.12. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

7.13. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, tais como a proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (Instrução Normativa SEGES/MPDG nº 3, de26 de abril de 2018 c/c Decreto estadual nº 67.608, de 2023).

7.14. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

7.15. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, paraque sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.16. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à extinção

contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

7.17. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, atéque se decida pela extinção do contrato, caso o contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

7.18. O pagamento será efetuado no prazo de 30 (trinta) dias, contados da apresentação da nota fiscal ou documento de cobrança equivalente, desde que tenha sido finalizada a liquidação da despesa, conforme seção anterior, nos termos do art. 2º, II, do Decreto estadual nº 67.608, de2023.

7.19. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente na forma da legislação aplicável (artigo 2º, inciso III, do Decreto estadual nº 67.608, de 2023, c/c o artigo 1º do Decreto estadual nº 32.117, de 1990), bem como incidirão juros moratórios, a razão de 0,5% (meio por cento) ao mês, calculados pro rata temporis, em relação ao atraso verificado.

Forma de pagamento

7.20. O pagamento será realizado por meio de ordem bancária, para depósito em conta corrente bancária em nome do contratado no Banco do Brasil S/A. 8.20.1. Constitui condição para a realização dos pagamentos a inexistência de registros em nome do contratado no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais– CADIN ESTADUAL”, o qual deverá ser consultado por ocasião da realização de cada pagamento. O cumprimento desta condição poderá se dar pela comprovação, pelo contratado, de que os registros estão suspensos, nos termos do artigo 8º da Lei estadual nº 12.799, de 2008.

7.21. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.22. O Contratante poderá, por ocasião do pagamento, efetuar a retenção de tributos determinada por lei, ainda que não haja indicação de retenção na nota fiscal apresentada ou que se refira a retenções não realizadas em meses anteriores.

7.22.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

7.23. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8. Critérios de seleção do fornecedor

Forma de seleção e critério de julgamento da proposta

8.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

Regime de Execução

8.2. O regime de execução do contrato será empreitada por valor global.

Exigências de habilitação

8.3. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

8.4. **Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei,tenha validade para fins de identificação em todo o território nacional;

8.5. **Empresário individual:** inscrição no Registro Público de Empresas Mercantis, a cargo da

Junta Comercial da respectiva sede;

8.6. **Microempreendedor Individual - MEI**: Certificado da Condição de Microempreendedor

Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

8.7. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI**: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

8.8. **Sociedade empresária estrangeira**: portaria de autorização de funcionamento no Brasil,

publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

8.9. **Filial, sucursal ou agência de sociedade simples ou empresária**: inscrição do ato

constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

8.10. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial, devendo o estatuto estar adequado à Lei nº 12.690, de 2012; documentos de eleição ou designação dos atuais administradores; e registro perante a entidade estadual da Organização das Cooperativas Brasileiras de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

8.11. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

8.12. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;
8.13. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria- Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à DívidaAtiva da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federaldo Brasil e da Procuradora-Geral da Fazenda Nacional.

8.14. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
8.15. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

8.16. Prova de inscrição no cadastro de contribuintes Estadual/Distrital e/ou Municipal/Distrita relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível como objeto contratual;

8.17. Prova de regularidade com a Fazenda *Municipal* do domicílio ou sede do fornecedor, relativaà atividade em cujo exercício contrata ou concorre;

8.18. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

8.19. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os

benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará

dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

8.20. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021 c/c Decreto estadual nº 67.608, de 2023), ou de sociedade simples;

8.21. certidão negativa de falência, recuperação judicial ou extrajudicial, expedida pelo distribuidor da sede do fornecedor;

8.21.1. Caso o fornecedor esteja em recuperação judicial ou extrajudicial, deverá ser comprovado o acolhimento do plano de recuperação judicial ou a homologação do plano de recuperação extrajudicial, conforme o caso;

8.22. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

8.22.1. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superioresa 1 (um);

8.22.2. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura (Lei nº 14.133, de 2021, art. 65, §1º);

8.22.3. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

8.22.4. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped, quando for o caso, ou outro limite estabelecido pela legislação aplicável;

8.22.5. Caso o licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação [capital mínimo OU patrimônio líquido mínimo] de 0,5% (meio por cento) do valor estimado da contratação;

Qualificação Técnica

9. Comprovação de capacidade operacional para execução de fornecimento similar de complexidade tecnológica e operacional equivalente ou superior ao objeto desta contratação, ou ao item pertinente, por meio da apresentação de certidão(ões) ou atestado(s), fornecido(s) por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

- Para fins da comprovação de que trata este subitem, o(s) atestado(s) ou certidão(ões) deverá(ão) dizer respeito a contrato(s) executado(s) com a(s) seguinte(s) característica(s) mínima(s):

- A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de solução de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets ou similar à proposta, em ambiente compatível ao da CONTRATANTE, contendo no mínimo 40.000 (quarenta mil) ativos monitorados.

- A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de solução de segurança e antivírus para servidores em cloud ou similar à proposta, em ambiente compatível ao da CONTRATANTE, contendo no mínimo 2.000 (dois mil) ativos monitorados.

- A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de solução de segurança antispam/mail gateway para e-mail ou similar à proposta, em ambiente compatível ao da CONTRATANTE, contendo no mínimo 15.000 (quinze mil) caixas postais monitoradas.

- A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de serviço de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets, em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano), em ambiente compatível ao da CONTRATANTE, contendo no mínimo 20.000 (vinte mil) ativos monitorados;

- A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de solução de monitoramento com, no mínimo, 250 (duzentos e cinquenta) ativos de rede, servidores e aplicações monitorados.

- A proponente deverá apresentar atestado(s) de bom desempenho anterior em contrato de fornecimento de solução de Service Desk para abertura e resolução de chamados de no mínimo, 750 (setecentos e cinquenta) usuários.

- Será admitida, para fins de comprovação de quantitativo mínimo de fornecimento similar, a apresentação e o somatório de diferentes certidões ou atestados de fornecimentos executados de forma concomitante.

- Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

- O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade do(s) atestado(s), apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

Qualificação Técnica Profissional

Requisitos de Experiência Profissional Os serviços de suporte e garantia referente a solução de segurança, deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços; Comprovação de o licitante possui, em seu quadro de funcionários, na data prevista para a entrega da proposta, profissional de nível superior ou outro devidamente reconhecido pela respectiva entidade profissional copetente e que seja certificado pelo fabricante dos produtos objeto desta licitação, e/ou a comprovação da disponibidade do profissional mediante contrato de prestação de

serviços, sem vinculo trabalhista e regido pela legislação Civil. Deverá apresentar a certificação do(s) técnico(s) mediante certificados emitidos pelo fabricante.

9. Estimativas do Valor da Contratação

Valor (R$): 374.853.788,73

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. O valor estimado total da contratação é de **R$ 374.853.788,73** (Trezentos e setenta e quatro milhões, oitocentos e cinquenta e três mil, setecentos e oitenta e oito reais e setenta e três centavos), conforme custos unitários apostos na tabela acima ou em Anexo do Edital. O valor estimado da contratação foi definido com observância do disposto no Decreto estadual nº 67.888, de 17 de agosto de 2023.

11. Adequação orçamentária

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Tesouro.
11.2. A contratação será atendida pela seguinte dotação:
I) Gestão/Unidade: [130222];
II) Fonte de Recursos: [001];
III) Programa de Trabalho: [20122131862160000];
IV) Elemento de Despesa: [339040];
V) Plano Interno: [130.103];

11.3. *A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação daLei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.*

12. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

ELIENE SUZANA VEIGA DE LIMA

Equipe de apoio

Assinou eletronicamente em 08/08/2024 às 16:21:07.

ROSEANI MORAES PEREIRA

Equipe de apoio

OTTO LUIZ CASTRO NUNES

Autoridade competente

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Planilha de controle IRP secretarias.xlsx (28.77 KB)

ANEXO I.1
Estudo Técnico Preliminar – ETP

1. Informações Básicas
Número do processo: 007.00023837/2024-15

2. Descrição da necessidade
Registro de Preços para futura e eventual contratação de licenças de software de segurança, incluindo serviços de instalação, configuração e suporte, treinamento e atualização do software.

2.1. Motivação/Justificativa

A presente contratação justifica-se por estar em consonância a todos os esforços já empreendidos para elevar os níveis de gestão e governança do ambiente de TI da Secretaria de Agricultura e Abastecimento do Estado de São Paulo, a adoção de mecanismos de segurança pertinentes irá convergir em melhorias com vistas a fornecer serviços de TI com alta disponibilidade, confiabilidade, solidez.
A Secretaria nos últimos anos, tem investido em importantes iniciativas na área de segurança, com intuito de atender às demandas comuns dos órgãos da administração pública estadual.
Dessa forma, o investimento constante em cibersegurança é uma forma de garantir que os órgãos de governo possam cumprir suas funções com eficiência, transparência e responsabilidade, sem colocar em risco os seus dados e os seus objetivos estratégicos.

Em face dessas dificuldades se faz necessária a contratação de solução coorporativa de forma a gerenciar todo o parque de microcomputadores através de uma central de gerenciamento e administração consolidada em uma única ferramenta.

A contratação dessas soluções é uma necessidade. Ela permitirá que esta Pasta não apenas enfrente os desafios atuais, mas também esteja preparado para os desafios futuros, garantindo a proteção de suas informações, a conformidade legal e a excelência operacional. Para tanto, alguns itens são de extrema relevância ao justificar o investimento necessário e levantado neste estudo.

- **Elevação da Gestão e Governança de TI**: A contratação alinha-se perfeitamente aos esforços contínuos desta Secretaria para aprimorar e otimizar a gestão e governança de seu ambiente de TI. Ao adotar soluções avançadas, buscamos não apenas modernizar sua infraestrutura, mas também garantir que as operações diárias sejam realizadas de maneira eficiente e segura.
- Conformidade com a LGPD: A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece padrões rigorosos para a proteção de dados pessoais. A solução de segurança proposta não apenas atende a esses requisitos, mas também garante que a Secretaria esteja sempre em conformidade, evitando penalidades e garantindo a confiança do público.

- **Modernização e Transformação digital:** Em uma era dominada pela tecnologia, é imperativo que as instituições governamentais se adaptem e evoluam. A adoção de Tecnologia da Informação e das Comunicações (TIC) é um passo crucial nessa direção, permitindo que a Secretaria de Agricultura atenda às demandas dinâmicas da sociedade contemporânea e ofereça serviços de alta qualidade.
- **Gestão de Dados Sensíveis:** A Secretaria de Agricultura não é apenas um órgão governamental; é o guardião da rica base de dados da agricultura do país. As informações sob sua custódia são inestimáveis e, portanto, devem ser protegidas com o mais alto nível de segurança, garantindo sua integridade e confidencialidade.
- **Ameaças Cibernéticas:** Vivemos em uma era digital, onde as ameaças cibernéticas são uma realidade constante. Ransomware, phishing e outros ataques podem causar danos irreparáveis. A adoção de soluções robustas de segurança é, portanto, não apenas desejável, mas absolutamente essencial.
- **Pandemia e Trabalho Remoto:** A pandemia da Covid-19 redefiniu a forma como trabalhamos. Com um aumento no trabalho remoto, os riscos associados a ataques cibernéticos também aumentaram. A solução proposta leva em consideração essa nova realidade, garantindo segurança mesmo em ambientes de trabalho distribuídos.
- **Proteção contra Malwares:** Malwares são uma ameaça omnipresente. Eles podem se infiltrar em sistemas, causar danos e até mesmo levar a perdas financeiras significativas. Uma solução de segurança robusta é a primeira linha de defesa contra essas ameaças, garantindo que os sistemas desta Pasta permaneçam imunes a eles.
- **Conformidade com Controles de Segurança Cibernética**: A segurança cibernética não é apenas sobre proteger contra ameaças, mas também sobre aderir a padrões e práticas recomendadas. A solução proposta está em total conformidade com os controles críticos de Segurança Cibernética preconizados pelo CIS, garantindo uma abordagem holística à segurança.
- **Impacto da Contaminação**: Qualquer contaminação ou invasão pode ter consequências catastróficas. Além das perdas tangíveis, há também perdas intangíveis, como a confiança e reputação da instituição. A solução proposta busca minimizar esses riscos, garantindo que a Secretaria de Agricultura e Abastecimento continue sendo uma instituição confiável e respeitada

3. Área requisitante

Área Requisitante	Responsável
Departamento de Gestão de Redes e Comunicação	Eliene Suzana Veiga de Lima

4. Necessidades de Negócio

Em um mundo cada vez mais digital, a Secretaria de Agricultura e Abastecimento precisa garantir a segurança e o compliance de suas informações e sistemas.

A necessidade de segurança é evidente. Esta Secretaria é responsável por proteger dados pessoais, dados sensíveis e sistemas críticos. Esses dados incluem informações sobre cidadãos, serviços disponíveis, atendimento e documentos. Um ataque cibernético poderia causar danos irreparáveis a esta Pasta, incluindo perda de dados, interrupção das operações e até mesmo danos financeiros.

A cibersegurança é essencial para proteger os dados e as informações dos órgãos de governo, que podem ser alvo de ataques cibernéticos com intenções criminosas, como roubo, fraude, espionagem ou sabotagem. Esses ataques podem comprometer a integridade, a confidencialidade e a disponibilidade dos dados, causando prejuízos financeiros, danos à reputação e riscos à segurança nacional.

Para evitar esses cenários, os órgãos de governo devem investir constantemente em cibersegurança, adotando medidas preventivas, corretivas e reativas para garantir a defesa dos seus sistemas, redes e dispositivos. Essas medidas incluem:

- **Segurança de rede:** para impedir o acesso não autorizado ou malicioso à rede de computadores do órgão de governo, utilizando firewalls, antivírus, criptografia e outras ferramentas.
- **Segurança de aplicativos:** para assegurar que os softwares e os dispositivos utilizados pelo órgão de governo estejam livres de vulnerabilidades e ameaças, seguindo boas práticas de desenvolvimento, teste e atualização.
- **Segurança de informações:** para preservar a integridade e a privacidade dos dados armazenados ou transmitidos pelo órgão de governo, definindo políticas de acesso, controle e backup dos dados.
- **Segurança operacional:** para estabelecer os processos e as decisões para o tratamento e a proteção dos dados do órgão de governo, determinando as permissões dos usuários, os procedimentos de armazenamento e compartilhamento dos dados e as normas de conduta e ética.
- **Recuperação de desastres e continuidade dos negócios:** para planejar como o órgão de governo irá responder a um incidente de cibersegurança ou a qualquer outro evento que cause a perda de operações ou dados, definindo as estratégias de restauração das atividades e das informações afetadas pelo incidente.
- **Educação do usuário final:** para conscientizar os funcionários e os gestores do órgão de governo sobre a importância da cibersegurança e as boas práticas de segurança, ensinandoos a evitar comportamentos que possam facilitar ataques cibernéticos, como abrir anexos suspeitos, usar senhas fracas ou conectar dispositivos não identificados.

A necessidade de proteção de dados também é importante. A Secretaria de Agricultura e Abastecimento está sujeita a uma série de leis e regulamentos, incluindo a Lei Geral de Proteção de Dados (LGPD). O não cumprimento dessas leis e regulamentos pode resultar em penalidades financeiras e danos à reputação. Os softwares de segurança oferecem proteção as informações e aos sistemas contra-ataques cibernéticos e vazamento de dados. Observando assim a adequação da entidade à lei nacional.

A adoção desses softwares permitirá que a Secretaria de Agricultura:
Garanta a segurança de suas informações e sistemas: Os softwares de segurança ajudarão a proteger suas informações e sistemas contra-ataques cibernéticos.
Esteja em conformidade com as leis e regulamentos: Os softwares de segurança ajudarão a estar em conformidade com as leis e regulamentos aplicáveis.
A adoção de novos e a continuação do uso de softwares de segurança é a chave para atender a essas necessidades e garantir a continuidade operacional desta Pasta.

5. **Necessidades Tecnológicas**

   As necessidades tecnológicas, também chamadas de requisitos da solução de tecnologia, descrevem as características de uma solução que atende aos requisitos do negócio são desenvolvidas e definidas neste documento após a realização de uma análise de requisitos. A segurança da informação – requisito essencial para a utilização de todos os serviços disponíveis - deve ser integrada à solução, com estratégia de proteção e conformidade de dispositivos, usuários, dados e aplicações, considerando o contexto de acesso, como uma ferramenta para segurança da informação capaz de fornecer serviços de:

   - Antivírus de arquivos residente (anti-spyware, anti-ransomware anti-trojan, AntiMalware etc.) que verifique qualquer arquivo criado, acessado ou modificado;
   - Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
   - Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
   - O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
   - Firewall com IDS;
   - Autoproteção (contra-ataques aos serviços / processos do antivírus);
   - Controle de dispositivos externos;
   - Controle de acesso a sites por categoria, por horário e por usuários, ex: Bloquear conteúdo adulto, sites de jogos etc.;
   - Controle de acesso a websites por dados, ex: Bloquear websites com conteúdo de vídeo e áudio;
   - Controle de execução de aplicativos;
   - Controle de vulnerabilidades do Windows e dos aplicativos instalados;

Solução de proteção contra ameaças avançadas, com funcionalidades de detecção, bloqueio, investigação e resposta a incidentes, incluindo console Web ou console gráfica do próprio fabricante para administração da solução e centralização de eventos;

6. **Demais requisitos necessários e suficientes à escolha da solução de TIC**

   6.1. Requisitos de Capacitação da solução de segurança

   - Cada módulo de treinamento deverá ser de no mínimo 16 horas de duração.
   - O treinamento deve ser realizado de segunda a sexta-feira (dias úteis), entre 8h (oito) horas e 18h (dezoito) horas.

- Para cada módulo da solução contratada, o treinamento oficial deverá ser efetuado pelo fabricante ou entidade credenciada com a emissão de certificados individuais para os colaboradores;
- Os treinamentos consistirão na capacitação de técnicos dos órgãos participantes do SRP nos processos de trabalho, métodos, técnicas e ferramentas integrantes da solução de segurança implantada;
- O mesmo deverá ser realizado, dentro da região de São Paulo ou remotamente, a critério da CONTRATANTE;
- Deverá ser emitido um certificado para cada participante do treinamento;
- Aceite por parte da CONTRATANTE.

6.2. Requisitos de Manutenção

- Devido às características da solução de segurança, há necessidade de realização de manutenções corretivas e evolutivas da solução de segurança pela CONTRATADA e pelo fabricante da solução de segurança, visando à manutenção da disponibilidade da solução;
- Os softwares da solução de segurança terão suas atualizações pelo prazo de validade de 60 (sessenta) meses.
- O serviço de suporte técnico da solução de segurança deverá ser de 60 (sessenta) meses prestado pelo fabricante em regime 24 x 7 x 365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) contra falhas e correções, disponibilizando as atualizações de versão e definição de vírus periodicamente.
- A CONTRATADA deverá fornecer e-mail, número telefônico e/ou opção via website para abertura de chamados técnicos, estes deverão possuir identificador (numérico) próprio, repassado ao CONTRATANTE, a fim de registro e acompanhamento das ocorrências.
- O suporte técnico prestado pela CONTRATADA consiste no esclarecimento de dúvidas, na reparação das eventuais falhas de funcionamento, mediante a substituição de versão, de acordo com os manuais e normas técnicas específicas do produto, bem como, orientação das melhores práticas de uso dos produtos adquiridos.
- Entende-se por término do atendimento, das ocorrências em aberto, a disponibilidade para uso em perfeitas condições de funcionamento no local onde está instalado, estando condicionado à aprovação do CONTRATANTE.
- Para a solução de segurança, uma vez registrada a ocorrência junto à CONTRATADA, ela será encaminhada para os procedimentos de atendimento e solução dos problemas, devendo ter como objetivos de atendimento os índices de criticidade determinados pelo FABRICANTE, descritos a seguir:

Criticidade	Descrição	Atendimento	Resolução do Atendimento

Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema, ou dos dados. Exemplo: Serviço inativo.	30 minutos a 1 hora	Menos de 4 horas
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade. a curto prazo, possa ser afetada negativamente. Exemplo: Servidor não responde a comandos ou responde com resultados inesperados. Arquivos de log corrompidos ou inexistentes.	4 a 6 horas	Menos de 10 horas
Severidade 3 (Baixa)	Demais problemas que não afetem diretamente o ambiente de produção. Exemplo: Problemas na geração de relatórios e dúvidas gerais de operação/configuração.	8 a 10 horas	Menos de 30 horas

- Além do atendimento nos níveis de criticidade citados no subitem anterior, a CONTRATANTE terá o direito de, no mínimo, 2 (duas) visitas técnicas anuais presenciais ou conforme acordado com a CONTRATANTE, para realização de serviço técnico de CyberSecurity Health Check com análise e validação de processos administrativos de segurança da infraestrutura dos softwares de segurança da CONTRATANTE de acordo com as melhores práticas do fabricante, realizadas por técnicos certificados e especialistas.

6.3. Requisitos da Implementação

A implantação da solução deve seguir as boas práticas de mercado no gerenciamento de projetos, bem como as boas práticas e diretrizes do FABRICANTE da solução.

Deverão observar integralmente os requisitos de projeto da solução de segurança e de implementação descritos a seguir:

- O cálculo de horas para suporte on-site de cada solução prevista, instalação e configuração das licenças dos softwares de segurança é de 15% (quinze por cento) da quantidade de licenças que serão contratadas, podendo ser adequada pela unidade CONTRATANTE (maior ou menor) de acordo com a necessidade.
- A CONTRATANTE, no momento da assinatura do contrato, deverá apresentar a certificação dos técnicos mediante certificados emitidos pelo fabricante da solução de segurança.
- Instalação e configuração total de todas as licenças do software de segurança adquirido no ambiente físico/virtual da CONTRATANTE, no prazo máximo de 45 (quarenta e cinco) dias após a emissão da ordem de serviço;
- É de responsabilidade da CONTRATADA a remoção remota da solução antiga de solução de segurança, atualmente instalada nos equipamentos da CONTRATANTE.

O projeto de implementação das licenças dos softwares de segurança deverá ser conduzido em etapas:

- Iniciação: a CONTRATADA deverá criar a visão do projeto e definirá o escopo de trabalho necessário para trazê-la para a realidade;
- Planejamento: deverá consistir na elaboração de um Plano Técnico a serem utilizados na implantação do projeto;
- Implementação: consistirá na execução das atividades definidas na fase de planejamento, podendo ser dividida em sub-bases para melhor controle;
- Estabilização: a solução deverá ser disponibilizada para os usuários do ambiente de produção, sendo efetuados os ajustes necessários para a estabilização dela;

- Encerramento: Deverá ser entregue a documentação do projeto, e coletada a aprovação formal do cliente;

Da inicialização e planejamento

- Reunião de startup;
- Apresentação dos requisitos necessários de infraestrutura para início do projeto;
- Definição e alinhamento de cronograma para implementação das soluções;
- Levantamento de informações do ambiente pertinentes ao projeto de implementação;
- Alinhamento de requisitos necessários para implementação das soluções;
- Levantamento de políticas e regras para planejamento, implementação e configurações solução de segurança;
- Definição de papéis e responsabilidades;
- O prazo para entrega da CONTRATADA do planejamento de implementação das soluções de segurança devem ser de no máximo 15 (quinze) dias da assinatura do contrato e a CONTRATANTE tem 5 (cinco) dias para dar o aceite no projeto;
- A partir da data de aceite, por parte da CONTRATANTE, ao projeto e cronograma entregues pela CONTRATADA. Esse prazo é referente às atividades da CONTRATADA. Não estarão aí contabilizadas as atividades de responsabilidade da CONTRATANTE;
- A CONTRATADA deverá apresentar um projeto para desinstalação remota da solução de segurança existente em toda a rede da CONTRATANTE.
- Não serão considerados responsabilidade da CONTRATADA implementação de agentes em equipamentos fora de pré-requisitos estabelecidos pelo fabricante e sem conectividade com a console central de administração da solução.

Da implementação da solução de segurança:

- Deverão acompanhar 30% de implementação nas dependências da CONTRATANTE em conjunto com a equipe de analistas de segurança da informação da CONTRATADA ou conforme acordado com a CONTRATANTE;
- O serviço de implementação preferencialmente será realizado nas dependências da CONTRATANTE, em horário comercial, das 08h00 às 18h00, de segunda a sexta-feira, excetuando-se feriados nacionais e estaduais ou conforme acordado com a CONTRATANTE. Quando se tratar de equipamentos críticos (servidores, storages, dispositivos móveis, entre outros), estas implementações poderão ser realizadas fora de horário comercial e/ou nos finais de semana.
- Instalação e configurações globais das consoles de administração da solução de segurança. Integração de todos os itens que compõem a solução de modo a permitir a visão e o gerenciamento em uma única console;
- Deverá ser utilizada como método de instalação (deploy) dos agentes nos equipamentos da CONTRATANTE, a instalação remota via console da solução contratada ou solução de distribuição similar sem custos adicionais. A CONTRATANTE fornecerá os prérequisitos para viabilidade da instalação remota via console da solução;
- Instalação (deploy) dos agentes da solução em servidores físicos e virtuais, incluindo remoção remota dos agentes existentes quando aplicável; Instalação (deploy) dos agentes da solução em desktops e notebooks, que fazem ou não parte do domínio local (Active

Directory), incluindo remoção remota dos agentes existentes quando aplicável, desde que possuam comunicação de rede com a rede principal da CONTRATANTE;
- Geração de pacotes de instalação (deploy), para a equipe da CONTRATANTE realizar a instalação da solução de segurança nos equipamentos que não possuem comunicação de rede com a rede principal da CONTRATANTE, incluindo remoção remota dos agentes existentes quando aplicável;
- Durante a fase de implementação a CONTRATADA deverá disponibilizar técnicos capacitados para acompanhamento em cada uma das equipes de implantação, com objetivo de resolver problemas de acesso físico e logico às localidades;
- À CONTRATADA ficará a cargo de efetuar a remoção remota prévia dos agentes em servidores devido a criticidade do ambiente;
- Criação de políticas de segurança em conjunto com as equipes técnicas da CONTRATANTE.

Do encerramento:
- Será considerada concluída a implementação da solução de segurança quando o número de equipamentos protegidos for igual ou superior a 60% do volume de equipamentos existentes.

Da estabilização:
- Deverão executar Health Check (saúde das consoles) nas soluções de segurança semestralmente, englobando:
- Validar as configurações do servidor da console de gerenciamento da solução de segurança;
- Validar as políticas da solução de segurança;
- Revisar a configuração da infraestrutura da solução de segurança;
- Criar um relatório que sugira melhorias com base nas melhores práticas da solução de segurança;

6.4. Requisitos da Contratação

Conforme análise da equipe, os requisitos da contratação abrangem o seguinte:

ITEM 01 - SOFTWARE DE SEGURANÇA E ANTIVÍRUS PARA SERVIDORES FÍSICOS, MICROCOMPUTADORES E SMARTPHONES/TABLETS COM DETECÇÃO E RESPOSTA E SOFTWARE DE ANTISPAM/PROTEÇÃO PARA O MICROSOFT OFFICE 365

6.4.1. Do módulo de proteção de endpoint
6.4.1.1. A solução proposta deverá proteger os sistemas operacionais para estações de trabalho:
6.4.1.1.1. Windows 7;
6.4.1.1.2. Windows 8;
6.4.1.1.3. Windows 8.1;
6.4.1.1.4. Windows 10;
6.4.1.1.5. Windows 11;
6.4.1.2. A solução proposta deverá proteger os sistemas operacionais para servidores:
6.4.1.2.1. Windows 7 Windows Small Business Server 2011;

6.4.1.2.2. Windows MultiPoint Server 2011;
6.4.1.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022;
6.4.1.3. A solução proposta deverá proteger os servidores de terminal Microsoft:
6.4.1.3.1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022;
6.4.1.4. A solução proposta deverá proteger os sistemas operacionais Linux:
6.4.1.4.1. Linux Mint 20.3 e posteriores (64bits);
6.4.1.4.2. Amazon Linux 2 (64bits);
6.4.1.4.3. CentOS 6.7 e posteriores (32/64bits);
6.4.1.4.4. Debian 11 e posteriores (32/64bits);
6.4.1.4.5. OpenSUSE Leap 15 (64bits);
6.4.1.4.6. Oracle Linux 7.3 e posteriores (64bits);
6.4.1.4.7. Red Hat Enterprise Linux 6.7 e posteriores (32/64bits);
6.4.1.4.8. SUSE Server 12.5 e posteriores (64bits);
6.4.1.4.9. Ubuntu 20.04 e posteriores (64bits);
6.4.1.4.10. Rocky Linux 8.5 e posteriores (64bits);
6.4.1.4.11. CentOS Stream 8 e posteriores (64bits);
6.4.1.4.12. Sistemas operacionais Arm de 64 bits: CentOS Stream 9, SUSE Linux Enterprise Server 15 e Ubuntu 22.04 LTS;
6.4.1.5. A solução proposta deverá proteger os sistemas operacionais MAC OS:
6.4.1.5.1. macOS 12 – 14;
6.4.1.6. Ferramentas de virtualização MAC OS:
6.4.1.6.1. Parallels Desktop 16 para Mac Business Edition;
6.4.1.6.2. VMware Fusion 11.5 Profissional;
6.4.1.6.3. VMware Fusion 12 Profissional;
6.4.1.7. A solução proposta deverá suportar as seguintes plataformas virtuais:
6.4.1.7.1. VMware Workstation 17.0.2 Pro;
6.4.1.7.2. VMware ESXi 8.0 Update 2;
6.4.1.7.3. Microsoft Hyper-V Server 2019;
6.4.1.7.4. Citrix Virtual Apps e Desktop 7 2308;
6.4.1.7.5. Citrix Provisioning 2308;
6.4.1.7.6. Citrix Hypervisor 8.2 Update 1;
6.4.2. Do módulo de gerenciamento avançado
6.4.2.1. A solução proposta deve suportar arquitetura cloud-native e On-premise;
6.4.2.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
6.4.2.2.1. Amazon Web Services;
6.4.2.2.2. Microsoft Azure;
6.4.2.3. A solução proposta deve incluir as seguintes opções de integração SIEM:
6.4.2.3.1. HP (Microfoco) ArcSight;
6.4.2.3.2. IBM Qradar;
6.4.2.3.3. Splunk;
6.4.2.3.4. Kaspersky KUMA;
6.4.2.4. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and response (MDR) e Anti-APT do próprio fornecedor,

para caça ativa a ameaças e resposta automatizada a incidentes;
6.4.2.5. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;
6.4.2.6. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos;
6.4.2.7. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede;
6.4.2.8. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros;
6.4.2.9. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador;
6.4.2.10. A solução proposta deve incorporar no sensor de endpoint distribuição /retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento;
6.4.2.11. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização;
6.4.2.12. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis;
6.4.2.13. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem;
6.4.2.14. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:
6.4.2.14.1. Status do dispositivo;
6.4.2.14.2. Tag;
6.4.2.14.3. Diretório ativo;
6.4.2.14.4. Proprietários de dispositivos;
6.4.2.14.5. Hardware;
6.4.2.15. A solução proposta deve suportar os seguintes canais de entrega de notificação:
6.4.2.15.1. E-mail;
6.4.2.15.2. Registro de sistema;
6.4.2.15.3. SMS;
6.4.2.16. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:
6.4.2.16.1. Atributos de rede;
6.4.2.16.2. Nome;
6.4.2.16.3. Domínio e/ou Sufixo de Domínio;
6.4.2.16.4. Endereço de IP;
6.4.2.16.5. Endereço IP para servidor de gerenciamento;
6.4.2.16.6. Localização no Active Directory;
6.4.2.16.7. Unidade organizacional;
6.4.2.16.8. Grupo;

6.4.2.16.9. Sistema operacional;
6.4.2.16.10. Número do pacote de serviço;
6.4.2.16.11. Arquitetura Virtual;
6.4.2.16.12. Registro de aplicativos;
6.4.2.16.13. Nome da Aplicação;
6.4.2.16.14. Versão do aplicativo;
6.4.2.16.15. Fabricante;
6.4.2.16.16. Tipo e versão;
6.4.2.16.17. Arquitetura;
6.4.2.17. 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 gestão;
6.4.2.18. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet /rede pública;
6.4.2.19. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:
6.4.2.19.1. Dispositivos Desktop/Servidores;
6.4.2.19.2. Dispositivos móveis;
6.4.2.19.3. Dispositivos de rede;
6.4.2.19.4. Dispositivos virtuais;
6.4.2.19.5. Componentes OEM;
6.4.2.19.6. Periféricos de computador;
6.4.2.19.7. Dispositivos IoT conectados;
6.4.2.19.8. Telefones VoIP;
6.4.2.19.9. Repositórios de rede;
6.4.2.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:
6.4.2.20.1. Nome da Aplicação;
6.4.2.20.2. Caminho do aplicativo;
6.4.2.20.3. Metadados do aplicativo;
6.4.2.20.4. Aplicativo Certificado digital;
6.4.2.20.5. Categorias de aplicativos predefinidas pelo fornecedor;
6.4.2.20.6. SHA256 e MD5;
6.4.2.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:
6.4.2.21.1. Bluetooth;
6.4.2.21.2. Dispositivos móveis;
6.4.2.21.3. Modems externos;
6.4.2.21.4. CD/DVD;
6.4.2.21.5. Câmeras e scanners;
6.4.2.21.6. MTPs;
6.4.2.21.7. E a transferência de dados para dispositivos móveis;
6.4.2.22. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização;

6.4.2.23. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão;
6.4.2.24. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:
6.4.2.24.1. Estruturas de domínios e grupos de trabalho do Windows;
6.4.2.24.2. Estruturas de grupos do Active Directory;
6.4.2.24.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador;
6.4.2.25. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização;
6.4.2.26. A solução proposta deve permitir realizar as seguintes ações para endpoints:
6.4.2.26.1. Verificação manual;
6.4.2.26.2. Verificação no acesso;
6.4.2.26.3. Verificação por demanda;
6.4.2.26.4. Verificação de arquivos compactados;
6.4.2.26.5. Verificação de arquivos individuais, pastas e unidades;
6.4.2.26.6. Bloqueio e verificação de scripts;
6.4.2.26.7. Proteção contra alteração de registros;
6.4.2.26.8. Proteção contra estouro de buffer;
6.4.2.26.9. Verificação em segundo plano/inativa;
6.4.2.26.10. Verificação de unidade removível na conexão com o sistema;
6.4.2.27. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou AntiMalware;
6.4.2.28. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas;
6.4.2.29. 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;
6.4.2.30. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc;
6.4.2.31. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração;
6.4.2.32. A solução proposta deve suportar Windows Failover Cluster ou compor com outra solução de alta disponibilidade;
6.4.2.33. A solução proposta deve ter um recurso de Clustering integrado;
6.4.2.34. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus;
6.4.2.35. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia;
6.4.2.36. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança;

6.4.2.37. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo;
6.4.2.38. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux;
6.4.2.39. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB;
6.4.2.40. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB;
6.4.2.41. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes;
6.4.2.42. A solução proposta deverá possuir controles para download de DLL e drivers;
6.4.2.43. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo específico de prevenção de intrusão;
6.4.2.44. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável;
6.4.2.45. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela popup, entrada de log);
6.4.2.46. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server;
6.4.2.47. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam 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;
6.4.2.48. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las;
6.4.2.49. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior;
6.4.2.50. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários;
6.4.2.51. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança AntiMalware através do servidor de administração;
6.4.2.52. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários;
6.4.2.53. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações AntiMalware instalados, e para distribuir notificações sobre eventos por e-mail;
6.4.2.54. A solução proposta deve permitir a instalação centralizada de aplicativos de

terceiros em todos ou em computadores selecionados;
6.4.2.55. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração;
6.4.2.56. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal;
6.4.2.57. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software AntiMalware e dados sobre inventário de hardware e software, licenciamento etc.;
6.4.2.58. 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 definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis;
6.4.2.59. A solução proposta deve permitir ao administrador personalizar relatórios;
6.4.2.60. 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;
6.4.2.61. A solução proposta deve permitir ao administrador definir um período após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor;
6.4.2.62. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento;
6.4.2.63. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento;
6.4.2.64. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico;
6.4.2.65. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos;
6.4.2.66. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
6.4.2.67. O servidor de gerenciamento primário 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 secundários;
6.4.2.68. A solução proposta deve suportar integração com solução APT;
6.4.2.69. A solução proposta deve suportar a integração com o serviço Managed Detection and response;
6.4.2.70. A solução proposta deve permitir instalar o modulo de gerenciamento On-premise nos seguintes sistemas operacionais:
6.4.2.70.1. Windows;
6.4.2.70.2. Linux;
6.4.2.71. A solução proposta deverá suportar os seguintes servidores de banco

de dados:
6.4.2.71.1. Sistemas operacionais Windows:
6.4.2.71.1.1. Microsoft SQL Server;
6.4.2.71.1.2. Microsoft Banco de dados SQL do Azure;
6.4.2.71.1.3. MySQL Standard e Enterprise;
6.4.2.71.1.4. MariaDB;
6.4.2.71.1.5. PostgreSQL;
6.4.2.71.2. Sistemas operacionais Linux:
6.4.2.71.2.1. MySQL;
6.4.2.71.2.2. MariaDB;
6.4.2.71.2.3. PostgreSQL;
6.4.2.72. A solução proposta deverá suportar as seguintes plataformas virtuais:
6.4.2.72.1. Sistemas operacionais Windows:
6.4.2.72.1.1. VMware vSphere 6.7 e 7.0;
6.4.2.72.1.2. Estação de trabalho VMware 16 Pro;
6.4.2.72.1.3. Servidor Microsoft Hyper-V 2012 de 64 bits;
6.4.2.72.1.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;
6.4.2.72.1.5. Microsoft Servidor Hyper -V 2016 de 64 bits;
6.4.2.72.1.6. Servidor Microsoft Hyper-V 2019 de 64 bits;
6.4.2.72.1.7. Servidor Microsoft Hyper-V 2022 de 64 bits;
6.4.2.72.1.8. Citrix XenServer 7.1 LTSR;
6.4.2.72.1.9. Citrix XenServer 8.x;
6.4.2.72.1.10. Oracle VM VirtualBox 6.x;
6.4.2.72.2. Sistemas operacionais Linux:
6.4.2.72.2.1. VMware vSphere 6.7, 7.0 e 8.0;
6.4.2.72.2.2. VMware Desktop 16 Pro e 17 Pro;
6.4.2.72.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits;
6.4.2.72.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;
6.4.2.72.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits;
6.4.2.72.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits;
6.4.2.72.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits;
6.4.2.72.2.8. Citrix XenServer 7.1 e 8.x;
6.4.2.72.2.9. Oracle VM VirtualBox 6.x e7.x;
6.4.3. A solução proposta deve suportar criptografia ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.3.1. A solução proposta deve suportar criptografia em vários níveis:
6.4.3.1.1. Criptografia completa do disco – incluindo disco do sistema;
6.4.3.1.2. Criptografia de arquivos e pastas;
6.4.3.1.3. Criptografia de mídia removível;
6.4.3.1.4. Gerenciamento de criptografia Bitlocker e MacOS Filevault2;
6.4.3.2. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
6.4.3.2.1. A criptografia de arquivos em unidades de computador locais;
6.4.3.2.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões;

6.4.3.2.3. A criação de listas criptografadas de pastas em unidades de computador locais;
6.4.3.3. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
6.4.3.3.1. Especificar uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis;
6.4.3.3.2. Configurar regras de criptografia para arquivos armazenados em unidades removíveis individuais;
6.4.3.4. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
6.4.3.4.1. A criptografia de todos os arquivos armazenados em unidades removíveis;
6.4.3.4.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis;
6.4.3.5. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia;
6.4.3.6. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis;
6.4.3.7. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado;
6.4.3.8. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido;
6.4.3.9. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais;
6.4.3.10. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia;
6.4.3.11. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados;
6.4.3.12. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema;

6.4.3.13. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco

criptografado;
6.4.3.14. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário;
6.4.3.15. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados;
6.4.3.16. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos;
6.4.3.17. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação;
6.4.3.18. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário;
6.4.3.19. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização;
6.4.3.20. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bitlocker;
6.4.3.21. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft Bitlocker, incluindo:
6.4.3.21.1. Uso do Trusted Platform Module e configurações de senha;
6.4.3.21.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível;
6.4.3.21.3. Uso de autenticação que exige entrada de dados em um ambiente de préinicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets);
6.4.3.22. A solução proposta deve suportar criptografia em Microsoft Surface Tablets;
6.4.4. A solução proposta deve suportar gerenciamento de sistemas próprio ou compor ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.4.1. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
6.4.4.1.1. Instalação remota de software de terceiros;
6.4.4.1.2. Relatórios sobre software e hardware existentes;
6.4.4.1.3. Monitoramento para instalação de software não autorizado;

6.4.4.1.4. Remoção de software não autorizado;
6.4.4.2. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados;
6.4.4.3. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints;
6.4.4.4. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade;
6.4.4.5. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando

/enviando automaticamente os patches necessários para os terminais;
6.4.4.6. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches;
6.4.4.7. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade;
6.4.4.8. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros;
6.4.4.9. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança;
6.4.4.10. A solução proposta deve permitir ao administrador aprovar atualizações;
6.4.4.11. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes;
6.4.4.12. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias;
6.4.4.13. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis;
6.4.4.14. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros;
6.4.4.15. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos;
6.4.4.16. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências);
6.4.4.17. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações;
6.4.4.18. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch;
6.4.4.19. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’;
6.4.4.20. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”;
6.4.4.21. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft;
6.4.4.22. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários;
6.4.4.23. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes;
6.4.4.24. A solução proposta deve apoiar a implantação do sistema operacional;
6.4.4.25. A solução proposta deve suportar Wake-on LAN e UEFI;
6.4.4.26. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server;
6.4.4.27. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades

aos computadores clientes sem instalar as atualizações;
6.4.4.28. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador;
6.4.4.29. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente;
6.4.4.30. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros;
6.4.4.31. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas;
6.4.4.32. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota;
6.4.4.33. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis;
6.4.4.34. A solução proposta deve permitir ao administrador utilizar uma única tarefa /trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros;
6.4.4.35. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
6.4.4.35.1. Inicie a instalação ao reiniciar ou desligar o computador;
6.4.4.35.2. Instale o gerador necessário todos os pré-requisitos do sistema;
6.4.4.35.3. Permitir a instalação de novas versões de aplicativos durante as atualizações;
6.4.4.35.4. Baixe atualizações para o dispositivo sem instalá-las;
6.4.4.36. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas;
6.4.4.37. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais;
6.4.4.38. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
6.4.4.38.1. CEF;
6.4.4.38.2. LEEF;
6.4.4.39. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais;
6.4.4.40. O relatório da solução proposta deve conter informações CVE;
6.4.4.41. A solução proposta deve suportar instalação de aplicações e software de terceiros;
6.4.5. Do módulo de gerenciamento simplificado
6.4.5.1. A solução proposta deve suportar arquitetura cloud;
6.4.5.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional;
6.4.5.3. O console de gerenciamento web da solução proposta deve ser simples de

usar e deve suportar dispositivos com tela sensível ao toque;
6.4.5.4. A solução proposta deve permitir ao administrador gerar relatórios prédefinidos;
6.4.5.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint;
6.4.5.6. A solução proposta deve atender as condições apontadas no item e subintes 1.1.6;
6.4.5.7. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS;
6.4.5.8. A solução proposta deve incluir informações do endpoint:
6.4.5.8.1. IP público de internet;
6.4.5.8.2. IP interno do dispositivo;
6.4.5.8.3. Versão do agente de proteção;
6.4.5.8.4. Última comunicação com a console, contendo data e hora;
6.4.5.8.5. Informações do sistema operacional;
6.4.5.9. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365 ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.5.10. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365 ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.5.11. A solução proposta deve incluir uma plataforma de capacitação online em segurança cibernética ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.6. A solução proposta deve prover as seguintes proteções ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.6.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
6.4.6.1.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados;
6.4.6.2. A solução proposta deve ser de um único fornecedor e suportar todos os módulos descritos neste termo de referência;
6.4.6.3. A solução proposta deve suportar integração com AntiMalware Scan Interface (AMSI);
6.4.6.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender;
6.4.6.5. A solução proposta deve suportar o subsistema Linux no Windows;
6.4.6.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
6.4.6.6.1. Proteção contra ameaças sem arquivos (Fileless);
6.4.6.7. Fornecimento de proteção baseada em machine learning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
6.4.6.8. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
6.4.6.9. A solução proposta deve fornecer varredura de memória do kernel para

estações de trabalho Linux.
6.4.6.10. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados;
6.4.6.11. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra-ataques remotos de criptografia;
6.4.6.12. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows;
6.4.6.13. A solução proposta deve fornecer análise comportamental baseada em machine learning;
6.4.6.14. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento;
6.4.6.15. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
6.4.6.15.1. Controles de aplicativos;
6.4.6.15.2. Controle web e dispositivos;
6.4.6.15.3. HIPS e Firewall;
6.4.6.15.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
6.4.6.15.5. Gerenciamento de criptografia de arquivos e discos;
6.4.6.15.6. Controle adaptativo para detecção de anomalias;
6.4.6.16. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor;
6.4.6.17. A solução proposta deve ser protegida por senha para evitar que o processo do AntiMalware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema;
6.4.6.18. A solução proposta deve ter bancos de dados de reputação locais e globais;
6.4.6.19. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares;
6.4.6.20. A solução proposta deve incluir um módulo capaz, no mínimo, de:
6.4.6.20.1. Bloqueio de aplicativos com base em sua categorização;
6.4.6.20.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos;
6.4.6.20.3. A adição de sub-redes e a modificação de permissões de atividade;
6.4.6.21. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização;
6.4.6.22. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção;
6.4.6.23. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses

arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça;
6.4.6.24. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
6.4.6.24.1. Modo silencioso;
6.4.6.24.2. Discos rígidos e dispositivos removíveis;
6.4.6.24.3. De todas as contas de usuários do dispositivo;
6.4.6.25. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
6.4.6.25.1. Exclusão imediata de dados;
6.4.6.25.2. Exclusão de dados adiada.
6.4.6.26. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
6.4.6.26.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
6.4.6.26.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.
6.4.6.27. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
6.4.6.28. A solução proposta deve suportar a tecnologia AM-PPL (AntiMalware Protected Process Light) para proteção contra ações maliciosas;
6.4.6.29. A solução proposta deve incluir proteção contra-ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo;
6.4.6.30. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário;
6.4.6.31. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem;
6.4.6.32. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas;
6.4.6.33. A solução proposta deve ser capaz de descriptografar e verificar o tráfego de rede transmitido por conexões criptografadas;
6.4.6.34. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
6.4.6.35. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
6.4.6.36. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint;
6.4.6.37. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem;
6.4.6.38. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir

uma ameaça detectada;
6.4.6.39. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa;
6.4.6.40. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior;
6.4.6.41. A solução proposta deve permitir que o administrador exclua arquivos/pastas /aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda;
6.4.6.42. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint;
6.4.6.43. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos ou compor ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.6.44. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos;
6.4.6.45. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo;
6.4.6.46. A solução proposta deve ter categoria de detecção para bloquear banners de sites;
6.4.6.47. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis ou compor ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.6.48. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos;
6.4.6.49. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais;
6.4.6.50. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP ou compor ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.6.51. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;
6.4.6.52. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões;
6.4.6.53. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos;
6.4.6.54. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem;
6.4.6.55. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração;
6.4.6.56. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões;
6.4.6.57. A solução proposta deve suportar o controle de scripts executados em

PowerShell;
6.4.6.58. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados;
6.4.6.59. A solução proposta deve ter a capacidade de controlar o acesso do sistema /aplicativo do usuário a dispositivos de gravação de áudio e vídeo;
6.4.6.60. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem;
6.4.6.61. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor;
6.4.6.62. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas;
6.4.6.63. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint;
6.4.6.64. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint ou compor ferramenta do mesmo fabricante que tenha capacidade similar com:
6.4.6.64.1. Filtro de anexos;
6.4.6.64.2. Verificação de mensagens de e-mail ao receber, ler e enviar;
6.4.6.65. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo;
6.4.6.66. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
6.4.6.67. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (Javascript, Visual Basic Script Scripts WSH (Javascript, Visual Basic Script etc.);
6.4.6.68. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware;
6.4.6.69. A solução proposta deve fornecer proteção contra-ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio;
6.4.6.70. A solução proposta deve incluir suporte ao protocolo IPv6;
6.4.6.71. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente;
6.4.6.72. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
6.4.6.72.1. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo;
6.4.6.72.2. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários;
6.4.6.73. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar;
6.4.6.74. A solução proposta deve incluir a verificação AntiMalware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos

protegidos por senha;
6.4.6.75. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística;
6.4.6.76. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail;
6.4.6.77. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária;
6.4.6.78. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows;
6.4.6.79. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados;
6.4.6.80. A solução proposta deve, ao detectar atividades semelhantes a ransomware /criptografia, bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça;
6.4.6.81. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft;
6.4.6.82. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização;
6.4.6.83. A solução proposta deve permitir a instalação de software com funcionalidades de AntiMalware e detecção e resposta de incidente a partir de um único pacote de distribuição;
6.4.6.84. A solução proposta deve suportar endereços IPv6;
6.4.6.85. A solução proposta deve suportar verificação em duas etapas (autenticação);
6.4.6.86. A solução proposta deve prever a instalação, atualização e remoção centralizada de software AntiMalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento;
6.4.6.87. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração;
6.4.6.88. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente;
6.4.6.89. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados AntiMalware mais recentes;
6.4.6.90. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de AntiMalware;
6.4.6.91. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas;
6.4.6.92. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas;
6.4.6.93. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos;
6.4.6.94. A solução proposta deve permitir o gerenciamento de componente que

controle a atividade do usuário na internet;
6.4.6.95. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi, Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor;
6.4.6.96. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes;
6.4.6.97. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS;
6.4.6.98. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentena em todos os recursos da rede onde o sensor de endpoint está instalado;
6.4.6.99. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração;
6.4.6.100. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos;
6.4.6.101. A solução proposta deve ter a capacidade de excluir atualizações baixadas;
6.4.6.102. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados;
6.4.6.103. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português;
6.4.6.104. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints;
6.4.6.105. A solução proposta deve incorporar funcionalidade de distribuição /retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos;
6.4.6.106. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou;
6.4.6.107. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor;
6.4.6.108. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional;
6.4.6.109. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor;
6.4.6.110. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
6.4.6.111. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível;
6.4.6.112. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica;
6.4.6.113. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados;
6.4.6.114. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado;

6.4.7. Do modulo de gerenciamento de dispositivos móveis
6.4.7.1. O modulo deve ser integrado a console de gerenciamento;
6.4.7.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
6.4.7.2.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition);
6.4.7.3. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
6.4.7.3.1. iOS 10–17 ou IPadOS 13–17;
6.4.7.4. A solução proposta deve oferecer suporte a dispositivos Android Device Owner;
6.4.7.5. A solução proposta deve suportar dispositivos iOS supervisionados;
6.4.7.6. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador;
6.4.7.7. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras;
6.4.7.8. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões;
6.4.7.9. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais);
6.4.7.10. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário;
6.4.7.11. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps;
6.4.7.12. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado;
6.4.7.13. A solução proposta deve ter recursos de conteinerização para dispositivos Android;
6.4.7.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
6.4.7.14.1. Dados em contêineres;
6.4.7.14.2. Contas de e-mail corporativo;
6.4.7.14.3. Configurações para conexão à rede Wi-Fi corporativa e VPN;
6.4.7.14.4. Nome do ponto de acesso (APN);
6.4.7.14.5. Perfil do Android for Wor;
6.4.7.14.6. Recipiente KNOX;
6.4.7.14.7. Chave do gerenciador de licença KNOX;
6.4.7.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
6.4.7.15.1. Todos os perfis de configuração instalados;
6.4.7.15.2. Todos os perfis de provisionamento;
6.4.7.15.3. O perfil iOS MDM;
6.4.7.15.4. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram

marcadas;
6.4.7.16. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo;
6.4.7.17. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:
6.4.7.17.1. Critérios de verificação do dispositivo;
6.4.7.17.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
6.4.7.18. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak etc.;
6.4.7.19. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
6.4.7.19.1. Cartões de memória e outras unidades removíveis;
6.4.7.19.2. Câmera do dispositivo;
6.4.7.19.3. Conexões Wi-Fi;
6.4.7.19.4. Conexões Bluetooth;
6.4.7.19.5. Porta de conexão infravermelha;
6.4.7.19.6. Ativação do ponto de acesso Wi-Fi;
6.4.7.19.7. Conexão de área de trabalho remota;
6.4.7.19.8. Sincronização de área de trabalho;
6.4.7.19.9. Definir configurações da caixa de correio do Exchange;
6.4.7.19.10. Configurar caixa de e-mail em dispositivos iOS MDM;
6.4.7.19.11. Configure contêineres Samsung KNOX;
6.4.7.19.12. Definir as configurações do perfil do Android for Work;
6.4.7.19.13. Configurar e-mail/calendário/contatos;
6.4.7.19.14. Defina as configurações de restrição de conteúdo de mídia;
6.4.7.19.15. Definir configurações de proxy no dispositivo móvel;
6.4.7.19.16. Configurar certificados e SCEP;
6.4.7.20. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay;
6.4.7.21. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
6.4.7.21.1. Google Play, Huawei App Gallery e Apple App Store;
6.4.7.21.2. Portal de inscrição móvel KNOX;
6.4.7.21.3. Pacotes de instalação pré-configurados independentes;
6.4.7.22. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel;
6.4.7.23. A solução proposta deve permitir que o PIN de um dispositivo móvel seja

redefinido remotamente;
6.4.7.24. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
6.4.7.24.1. VMware AirWatch 9.3 ou posterior;
6.4.7.24.2. MobileIron 10.0 ou posterior;
6.4.7.24.3. IBM MaaS360 10.68 ou posterior;
6.4.7.24.4. Microsoft Intune 1908 ou posterior;
6.4.7.24.5. SOTI MobiControl 14.1.4 (1693) ou posterior;
6.4.7.25. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo;
6.4.7.26. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
6.4.7.26.1. Google Play;
6.4.7.26.2. Galeria de aplicativos Huawei;
6.4.7.26.3. Loja de aplicativos da Apple;
6.4.7.27. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo;
6.4.7.28. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo;
6.4.7.29. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento;
6.4.7.30. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena;
6.4.7.31. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos;
6.4.7.32. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente;
6.4.7.33. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores;
6.4.7.34. A solução proposta deve fornecer funcionalidade Anti-roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente;
6.4.7.35. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel;
6.4.7.36. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis;
6.4.7.37. A solução proposta deve ter a capacidade de enviar aplicações recomendadas /exigidas pelo administrador para o dispositivo móvel;
6.4.7.38. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido;
6.4.7.39. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
6.4.7.40. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

6.4.8. Do módulo de EDR
6.4.8.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta;
6.4.8.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados;
6.4.8.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
6.4.8.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
6.4.8.5. Deve apresentar informações detalhadas contendo:
6.4.8.5.1. Usuário que executou a ação;
6.4.8.5.2. Informações acesso privilegiado;
6.4.8.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas;
6.4.8.7. A solução proposta deve suportar integração com serviço de reputação em nuvem;
6.4.8.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações etc.);
6.4.8.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único);
6.4.8.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;
6.4.8.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem;
6.4.8.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção;
6.4.8.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta;
6.4.8.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados;
6.4.8.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador;
6.4.8.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede;
6.4.8.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas;
6.4.8.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC;

6.4.8.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint;
6.4.8.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
6.4.8.20.1. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque);
6.4.8.20.2. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional;
6.4.8.20.3. Informações gerais sobre a detecção, incluindo modo de detecção;
6.4.8.20.4. Alterações no registro associadas à detecção;
6.4.8.20.5. Histórico da presença de arquivos no dispositivo;
6.4.8.20.6. Ações de resposta executadas pela aplicação;
6.4.8.21. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.;
6.4.8.22. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
6.4.8.22.1. Processo;
6.4.8.22.2. Conexões de rede;
6.4.8.22.3. Alterações no registro;
6.4.8.22.4. Detalhes do download de objeto;
6.4.8.23. A solução proposta deve fornecer orientação de resposta (resposta guiada);
6.4.8.24. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente;
6.4.8.25. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
6.4.8.25.1. Impedir a execução de objetos
6.4.8.25.2. Isolamento de host
6.4.8.25.3. Excluir objeto do host ou grupo de hosts
6.4.8.25.4. Encerrar um processo no dispositivo
6.4.8.25.5. Colocar um objeto em quarentena
6.4.8.25.6. Execute a verificação do sistema
6.4.8.25.7. Execução remota de programa/processo/comando
6.4.8.25.8. Iniciar a varredura IoC para um grupo de hosts.
6.4.9. Requisitos para documentação da solução.
6.4.9.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
6.4.9.1.1. Ajuda on-line para administradores;
6.4.9.1.2. Ajuda on-line para melhores práticas de implementação;
6.4.9.1.3. Ajuda on-line para proteção de servidores de administração;
6.4.9.2. A documentação do software AntiMalware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software AntiMalware;
6.4.9.3. Deve estar disponível página com informações de ciclo de vida das soluções e módulos.

6.4.10. Da Proteção para o Microsoft Office 365
6.4.10.1. Características Gerais ou compor ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.10.1.1. A solução deve ser entregue no modelo de “Software as a Service”, onde servidor e console administrativa são hospedados na nuvem;
6.4.10.1.2. Acesso a console administrativa via HTTPS;
6.4.10.1.3. A integração com o Office 365 deve ser realizada via API;
6.4.10.1.4. A autenticação da integração deve ser realizada via protocolo seguro OAuth 2.0;
6.4.10.1.5. A solução deve prover módulos de proteção para a suíte Microsoft Office 365 (Exchange Online, OneDrive, SharePoint e Teams);
6.4.10.1.6. A console deve prover painel de informações exibindo as informações principais da operação e do estado dos componentes de proteção;
6.4.10.1.7. Capacidade de geração de relatórios em no mínimo formato “.pdf”;
6.4.10.1.8. Capacidade de geração de relatório instantâneo;
6.4.10.1.9. Capacidade de agendamento automático de relatórios;
6.4.10.1.10. A solução deve verificar o tráfego de e-mails inbound e outbound;
6.4.10.1.11. Deve possuir quarentena para armazenar artefatos detectados como maliciosos;
6.4.10.1.12. A quarentena deve possuir no mínimo as seguintes opções:
6.4.10.1.12.1. Exibir detalhes do item;
6.4.10.1.12.2. Excluir item;
6.4.10.1.12.3. Liberar item;
6.4.10.1.12.4. Filtrar itens;
6.4.10.1.12.5. Salvar item em disco;
6.4.10.1.13. A gestão da solução deve ser realizada por usuário com perfil de administrador;
6.4.10.1.14. Deve ser possível atribuir perfil de administrador para um usuário na console de administração;
6.4.10.1.15. Deve ser capaz de detectar informação sensível em texto e imagens transmitidos e armazenados através da plataforma e alertar o administrador quanto ao risco de vazamento da informação;
6.4.10.2. Módulo de Proteção - AntiMalware
6.4.10.2.1. Deve proteger as caixas de correio contra vírus, Worms, trojans, entre outras ameaças que podem ser enviadas via e-mail.
6.4.10.2.2. Análise das ameaças deve ser realizada por no mínimo as seguintes tecnologias:
6.4.10.2.2.1. Assinaturas;
6.4.10.2.2.2. Heurística;
6.4.10.2.2.3. Comportamento;
6.4.10.2.2.4. Consulta ao repositório de inteligência do fabricante.
6.4.10.2.3. Capacidade de detectar ataques conhecidos e desconhecidos.
6.4.10.2.4. Ao detectar um malware, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:
6.4.10.2.4.1. Excluir a mensagem e colocá-la em quarentena;
6.4.10.2.4.2. Excluir anexo infectado e colocá-lo em quarentena;

6.4.10.2.4.3. Colocar tag no assunto;
6.4.10.2.4.4. Substituir arquivo por mensagem personalizada;
6.4.10.2.5. Notificar ao administrador sobre novas ameaças encontradas;
6.4.10.2.6. Notificar ao proprietário da caixa sobre mensagens excluídas;
6.4.10.2.7. Deve analisar arquivos nas seguintes aplicações:
6.4.10.2.7.1. Exchange Online;
6.4.10.2.7.2. OneDrive;
6.4.10.2.7.3. SharePoint;
6.4.10.2.7.4. Teams;
6.4.10.2.8. Oferecer proteção contra-ataques mailsploit, ghost spoofing e injeções de código malicioso;
6.4.1.1. Módulo de Proteção – Anti-Phishing

6.4.10.2.9. Deve proteger as caixas de correio contra phishing e links maliciosos enviados em mensagens de e-mail, evitando assim infecção por malware, roubo de dados pessoas e acesso a sites fraudulentos.
6.4.10.2.10. Deve validar o conteúdo das mensagens para detectar phishing, utilizando as seguintes tecnologias:
6.4.10.2.10.1. SPF (Sender Policy Framework);
6.4.10.2.10.2. DKIM (Domain-based Message Authentication);
6.4.10.2.10.3. DMARC (Domain-based Message Authentication, Reporting and Conformance);
6.4.10.2.10.4. Consulta ao repositório de inteligência do fabricante;
6.4.10.2.11. Capacidade de detectar ataques conhecidos e desconhecidos;
6.4.10.2.12. Ao detectar um link de phishing, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:
6.4.10.2.12.1. Excluir a mensagem e colocá-la em quarentena;
6.4.10.2.12.2. Permitir;
6.4.10.2.12.3. Mover para pasta “Lixo eletrônico”;
6.4.10.2.12.4. Colocar tag no assunto;
6.4.10.2.13. Notificar ao administrador sobre novas mensagens encontradas;
6.4.10.2.14. Notificar ao proprietário da caixa sobre mensagens excluídas;
6.4.10.2.15. Permitir a criação de exclusões por e-mail completo ou máscara.
6.4.10.3. Módulos de proteção - AntiSpam / Mass Mail
6.4.10.3.1. Deverá proteger todas as caixas de correio contra e-mail não solicitados “SPAM” e e-mails enviados em massa;
6.4.10.3.1.1. A verificação deve ser realizada através dos seguintes métodos:
6.4.10.3.1.2. Verificação de cabeçalho, conteúdo, anexos e elementos de design;
6.4.10.3.1.3. Algoritmos linguísticos e heurísticos;
6.4.10.3.1.4. Consulta ao repositório de inteligência do fabricante;
6.4.10.3.2. Ao detectar um SPAM, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:
6.4.10.3.2.1. Permitir;
6.4.10.3.2.2. Mover para a pasta “Lixo eletrônico”;
6.4.10.3.2.3. Colocar tag no assunto;
6.4.10.3.2.4. Notificar ao administrador sobre novas ameaças encontradas;

6.4.10.3.2.5. Notificar ao proprietário da caixa sobre mensagens excluídas;
6.4.10.3.2.6. Permitir a criação de exclusões por e-mail completo ou máscara;
6.4.10.4. Módulo de proteção - Filtro de conteúdo
6.4.10.4.1. Deve possibilitar a filtragem de anexos em mensagens de e-mail;
6.4.10.4.2. Capacidade de detectar anexos pelos seguintes parâmetros:
6.4.10.4.2.1. Formato do arquivo;
6.4.10.4.2.2. Nome completo do arquivo;
6.4.10.4.2.3. Nome do arquivo com máscara;
6.4.10.4.2.4. Arquivos MS Office com macro;
6.4.10.4.3. Ao detectar um anexo que se encaixe em uma das regras, a solução deve possibilitar as seguintes ações:
6.4.10.4.3.1. Excluir mensagem e colocá-la em quarentena;
6.4.10.4.3.2. Excluir anexo e colocá-lo em quarentena;
6.4.10.4.3.3. Permitir;
6.4.10.4.3.4. Colocar tag no assunto;
6.4.10.4.3.5. Substituir arquivo por mensagem personalizada;
6.4.10.4.3.6. Notificar ao administrador sobre novas ameaças encontradas;
6.4.10.4.3.7. Notificar ao proprietário da caixa sobre mensagens excluídas;
6.4.10.4.3.8. Permitir a criação de exclusões por e-mail completo ou máscara.

ITEM 02 - SOFTWARE DE SEGURANÇA E ANTIVÍRUS PARA AMBIENTES VIRTUALIZADOS ON PREMISE

6.4.11. Requerimentos para gerenciamento, administração e relatórios Centralizados

6.4.11.1. Permitir a instalação de software AntiMalware a partir de um único pacote de distribuição;
6.4.11.2. Deve ter perfis de instalação personalizáveis dependendo do número de nós protegidos;
6.4.11.3. Suportar endereços IPv6.
6.4.11.4. Suportar verificação em duas etapas (autenticação);
6.4.11.5. Deve ter capacidade de ler informações do AD para obter dados sobre contas de computadores na organização;
6.4.11.6. Deverá incluir uma consola web incorporada para a gestão dos Endpoints, que não deverá necessitar de qualquer instalação adicional;
6.4.11.7. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos de tela sensível ao toque;
6.4.11.8. Deve distribuir automaticamente as contas de computador por grupo de gerenciamento se novos computadores aparecerem na rede;
6.4.11.9. 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 AD;
6.4.11.10. Deverá prever a instalação, atualização e remoção centralizada de software AntiMalware, bem como configuração, administração e visualização centralizada de relatórios e

informações estatísticas sobre o seu funcionamento;
6.4.11.11. Deverá contemplar a remoção centralizada (manual e automática) de aplicativos incompatíveis do centro de administração;
6.4.11.12. Deverá 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;
6.4.11.13. Deverá permitir a instalação remota de software AntiMalware com as bases de dados AntiMalware mais recentes;
6.4.11.14. Deve permitir a atualização automática do software AntiMalware e das bases de dados AntiMalware;
6.4.11.15. Deve possibilitar o gerenciamento de um componente que proíba a instalação e /ou execução de programas;
6.4.11.16. Deve oferecer suporte à integração de API nativa com o Microsoft Azure e Google Cloud Platform;
6.4.11.17. Deve oferecer suporte à integração nativa da API com o ambiente de nuvem Amazon AWS, que inclui autenticação e localização de dispositivos usando a API AWS
6.4.11.18. Deve oferecer suporte à instalação remota de proteção usando API na AWS;
6.4.11.19. O servidor de gerenciamento centralizado da solução exibe recursos específicos da AWS (propriedades do dispositivo cliente, hierarquia de grupos de administração, Diretório AWS, assistente de configuração de proteção de segmento de nuvem e sondagem de segmento de nuvem) em sua interface;
6.4.11.20. Deve oferecer suporte a esquemas de licenciamento BYOL e PAYGo para proteção de nuvem pública;
6.4.11.21. Deve possibilitar o gerenciamento de um componente controlando o trabalho com dispositivos de E/S externos;
6.4.11.22. Deve possibilitar o gerenciamento de um componente que controla a atividade do usuário na internet;
6.4.11.23. 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;
6.4.11.24. 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;
6.4.11.25. 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;
6.4.11.26. 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;
6.4.11.27. Deve dar acesso aos serviços de nuvem do fornecedor de segurança AntiMalware por meio do servidor de administração;
6.4.11.28. Deve incluir a distribuição automática de licenças nos computadores clientes;
6.4.11.29. Deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários;

6.4.11.30. Deve ter um mecanismo de notificação para informar os usuários sobre eventos no software AntiMalware instalado e nas configurações, e para distribuir notificações sobre eventos via e-mail;
6.4.11.31. Permitir a instalação centralizada de aplicativos de terceiros em todos ou em alguns computadores;
6.4.11.32. 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.
6.4.11.33. Capacidade de especificar qualquer computador da organização como um centro de encaminhamento de eventos do agente AntiMalware 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;
6.4.11.34. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software AntiMalware, e dados sobre o inventário de hardware e software, licenciamento, etc.;
6.4.11.35. Deve ser capaz de exportar relatórios para arquivos PDF e XML;
6.4.11.36. Deve fornecer a administração centralizada de armazenamentos de backup e quarentena em todos os recursos de rede onde o software AntiMalware está instalado;
6.4.11.37. Deve prever a criação de contas internas para autenticar administradores no servidor de administração;
6.4.11.38. Deve prever a criação de uma cópia de backup do sistema de administração com o auxílio de ferramentas integradas do sistema de administração;
6.4.11.39. Deve oferecer suporte ao Windows Failover Cluster ou compor com outra solução de alta disponibilidade;
6.4.11.40. Deve ter um recurso de cluster integrado;
6.4.11.41. Deve incluir alguma forma de sistema para controlar epidemias de vírus;
6.4.11.42. 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;
6.4.11.43. O servidor de gerenciamento da solução deve incluir funções de segurança pré-definidas para Auditor, Supervisor e Agente de Segurança;
6.4.11.44. Capacidade de gerenciar dispositivos móveis por meio de comandos remotos;
6.4.11.45. Capacidade de excluir as atualizações baixadas;
6.4.11.46. Deve gerar atualizações do Servidor de Administração de Gerenciamento a partir da interface do aplicativo;
6.4.11.47. Deve permitir a seleção de um agente de atualização para computadores clientes com base em uma análise de rede;
6.4.11.48. O servidor de gerenciamento da solução 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;
6.4.11.49. O servidor de gerenciamento da solução 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:
6.4.11.49.1. Status do dispositivo;

6.4.11.49.2. Tag;
6.4.11.49.3. Diretório ativo;
6.4.11.49.4. Proprietários de dispositivos;
6.4.11.49.5. Hardware;
6.4.11.50. Suportar os seguintes canais de entrega de notificação:
6.4.11.50.1. E-mail;
6.4.11.50.2. Syslog;
6.4.11.51. 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;
6.4.11.52. Capacidade de realizar inventário em scripts e arquivos. arquivos dll;
6.4.11.53. Deve ter a capacidade de etiquetar/marcar computadores com base em:
6.4.11.53.1. Atributos de rede;
6.4.11.53.2. Nome;
6.4.11.53.3. Domínio e/ou Sufixo de Domínio;
6.4.11.53.4. IP;
6.4.11.53.5. Endereço IP para o servidor de gerenciamento;
6.4.11.53.6. Localização no Active Directory;
6.4.11.53.7. Unidade organizacional;
6.4.11.53.8. Grupo;
6.4.11.53.9. Sistema operacional;
6.4.11.53.10. Tipo e versão;
6.4.11.53.11. Arquitetura;
6.4.11.53.12. Número do pacote de serviço;
6.4.11.53.13. Arquitetura virtual;
6.4.11.53.14. Registro de aplicativos;
6.4.11.53.15. Nome da Aplicação;
6.4.11.53.16. Versão do aplicativo;
6.4.11.53.17. Fabricante;
6.4.11.54. A solução 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;
6.4.11.55. Deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectando pela internet/rede pública;
6.4.11.56. 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 definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis;
6.4.11.57. Ter um painel personalizável gerando e exibindo estatísticas em tempo real para endpoints;
6.4.11.58. Deve permitir que o administrador personalize os relatórios;
6.4.11.59. Deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado;
6.4.11.60. Deve permitir que o administrador estabeleça um período após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados são

excluídos automaticamente do servidor;
6.4.11.61. A solução deve permitir ao administrador criar categorias/grupos de aplicação com base em:
6.4.11.61.1. Nome da Aplicação;
6.4.11.61.2. Caminho do Aplicativo;
6.4.11.61.3. Metadados do aplicativo;
6.4.11.61.4. Aplicativo certificado digital;
6.4.11.61.5. Categorias de aplicativos pré-definidas pelo fornecedor;
6.4.11.61.6. SHA;
6.4.11.62. Computadores de referência para permitir/negar sua execução em endpoints;
6.4.11.63. Permitir que o administrador defina diferentes condições de alteração de status para grupos de endpoints no servidor de gerenciamento;
6.4.11.64. Permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento;
6.4.11.65. Deve ter um recurso/módulo embutido para coletar remotamente os dados necessários para solução de problemas dos endpoints, sem exigir acesso físico;
6.4.11.66. 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;
6.4.11.67. 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;
6.4.11.68. Deve possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:
6.4.11.68.1. Estruturas de domínios e grupos de trabalho do Windows;
6.4.11.68.2. Estruturas de grupos do AD;
6.4.11.68.3. Conteúdo de um arquivo de texto criado pelo administrador manualmente;
6.4.11.68.4. Ambiente AWS;
6.4.11.69. A solução 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;
6.4.11.70. As informações sobre o equipamento devem ser atualizadas após cada nova pesquisa de rede. A lista de equipamentos detectados deve abranger o seguinte:
6.4.11.70.1. Dispositivos;
6.4.11.70.2. Dispositivos móveis;
6.4.11.70.3. Dispositivos de rede;
6.4.11.70.4. Dispositivos virtuais;
6.4.11.70.5. Componentes OEM;
6.4.11.70.6. Periféricos de computador;
6.4.11.70.7. Dispositivos conectados;
6.4.11.70.8. Telefones VoIP;
6.4.11.70.9. Repositórios de rede;
6.4.11.71. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede;

6.4.11.72. A funcionalidade 'Device is Write Off' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos;
6.4.11.73. A solução deve incorporar um único agente de distribuição/retransmissão para dar suporte a pelo menos 10.000 endpoints para a entrega de proteção, atualizações, patches e pacotes de instalação para sites remotos;
6.4.11.74. 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;
6.4.11.75. Deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização;
6.4.11.76. Deve suportar OPEN API e incluir diretrizes para integração com sistemas externos de terceiros;
6.4.11.77. A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem a necessidade de acesso físico ao computador;
6.4.11.78. A solução proposta deve incluir Controle de Acesso Baseado em Função (RBAC) com funções predefinidas personalizáveis;
6.4.11.79. O servidor de gerenciamento primário/pai da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem;
6.4.11.80. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou;
6.4.11.81. O relatório da solução 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;
6.4.11.82. O servidor de gerenciamento principal deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade etc., dos terminais gerenciados dos servidores de gerenciamento secundário;
6.4.11.83. 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;
6.4.11.84. A solução deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional;
6.4.11.85. Deve permitir uma migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor;
6.4.11.86. Deve incluir a opção de integração SIEM – Syslog;
6.4.11.87. Deve incluir suporte para implantação baseada em nuvem por meio de:
6.4.11.87.1. Amazon Web Services;
6.4.11.87.2. Microsoft Azure;
6.4.11.88. Deve fornecer mecanismos de atualização de banco de dados AntiMalware, incluindo:
6.4.11.88.1. Múltiplas formas de atualização, incluindo canais de comunicação globais sobre o protocolo HTTPS, recurso compartilhado na rede local e mídia removível;
6.4.11.88.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica;
6.4.11.89. A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos;

6.4.12. Requisitos para antivírus em ambientes virtualizados baseado em agente

para Windows;

6.4.12.1. Oferecer suporte aos seguintes sistemas operacionais:
6.4.12.1.1. Windows 11 21H2 Pro/ Enterprise/ Education;
6.4.12.1.2. Windows 10 Desktop Pro 19H1/19H2/20H1/20H2/21H1 (32 / 64-bit);
6.4.12.1.3. Windows 10 Enterprise 2016 LTSC/2019 LTSC/19H1/19H2/20H1/20H2/21H1 (32 / 64-bit);
6.4.12.1.4. Windows 8.1 Update 1 Professional/Enterprise (32 / 64-bit);
6.4.12.1.5. Windows 7 Professional/Enterprise SP1 (32/64-bit);
6.4.12.1.6. Windows Server 2022 Standard/ Datacenter /Essentials (Desktop experience /Core);
6.4.12.1.7. Windows Server 2019 Standard/ Datacenter (Desktop experience/Core);
6.4.12.1.8. Windows Server 2016 Standard/ Datacenter (Desktop experience/Core);
6.4.12.1.9. Windows Server 2012 R2 Standard/ Datacenter /Essentials (Desktop experience/Core);
6.4.12.1.10. Windows Server 2012 Standard/ Datacenter /Essentials (Desktop experience /Core);
6.4.12.1.11. Windows Server 2008 R2 SP1 Standard/Enterprise/ Datacenter (Desktop experience/Core);
6.4.12.2. Características:
6.4.12.2.1. Oferecer suporte à verificação de objetos quando eles são acessados;
6.4.12.2.2. Suporte a verificações dos seguintes objetos:
6.4.12.2.2.1. Arquivos;
6.4.12.2.2.2. Fluxos alternativos do sistema de arquivos (fluxos NTFS);
6.4.12.2.2.3. Registro de inicialização e setores de inicialização em discos rígidos locais e unidades removíveis;
6.4.12.2.3. Suportar varredura sob demanda para executar 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;
6.4.12.2.4. 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;
6.4.12.2.5. Deve oferecer suporte a pastas compartilhadas de proteção em dispositivos contra criptografia maliciosa, bloqueando hosts que mostram atividade maliciosa;
6.4.12.2.6. Deve controlar a execução de scripts usando tecnologias de script do Microsoft Windows;
6.4.12.2.7. 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;
6.4.12.2.8. Deve verificar o tráfego de rede em busca de atividades típicas de ataques de rede e bloquear a atividade de rede do computador atacante;
6.4.12.2.9. 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;

6.4.12.2.10. 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;
6.4.12.2.11. Deve colocar em quarentena os objetos provavelmente infectados, movendoos 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;
6.4.12.2.12. Armazenar cópias criptografadas de objetos classificados como infectados no backup antes de desinfetá-los ou excluí-los;
6.4.12.2.13. Oferecer suporte a notificações do usuário;
6.4.12.2.14. Oferecer suporte à importação e exportação de configurações;
6.4.12.2.15. 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;
6.4.12.2.16. Deve oferecer suporte à proteção de memória contra explorações;
6.4.12.2.17. Deve suportar dispositivo de gerenciamento com a solução instalada via console de nuvem;
6.4.12.2.18. Fornecer integração com os mesmos fornecedores de Detecção de Endpoint e Resposta “EDR”, para busca ativa de ameaças e automação de resposta a incidentes;
6.4.13. Requisitos para antivírus em ambientes virtualizados baseado em agente para Linux;
6.4.13.1. A solução deve oferecer suporte aos seguintes sistemas operacionais:
6.4.13.1.1. CentOS 7.3 e posteriores (64-bit);
6.4.13.1.2. Debian GNU/Linux 9.4 e posteriores (32/64-bit);
6.4.13.1.3. Oracle Linux 7.3 e posteriores (64-bit);
6.4.13.1.4. Red Hat Enterprise Linux Server 7.3 e posteriores (64-bit);
6.4.13.1.5. SUSE Linux Enterprise Server 15 SP2 (64-bit);
6.4.13.1.6. Ubuntu 18.04 LTS e posteriores (64-bit);
6.4.13.2. Características:
6.4.13.2.1. 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;
6.4.13.2.2. Oferecer suporte a varredura de objetos do sistema de arquivos em tempo real e sob demanda;
6.4.13.2.3. Deve oferecer suporte a digitalização de objetos de inicialização, setores de inicialização, processo e memória do kernel;
6.4.13.2.4. Suportar neutralizar ameaças detectadas em arquivos e escolher automaticamente qual ação executar para neutralizar a ameaça;
6.4.13.2.5. Oferecer suporte ao armazenamento de cópias de backup de arquivos antes da desinfecção ou exclusão e restauração de arquivos de cópias de backup;
6.4.13.2.6. Oferecer suporte à notificação do administrador sobre eventos ocorridos durante a operação;
6.4.13.2.7. 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;
6.4.13.2.8. Suporte à adição de chaves, bem como à ativação usando códigos de ativação;
6.4.13.2.9. Suporte ao gerenciamento de um firewall do sistema operacional;

6.4.13.2.10. Suporte à proteção de seus arquivos nos diretórios locais com acesso à rede por protocolos SMB/NFS contra criptografia maliciosa remota;
6.4.13.2.11. Suporte à verificação de tráfego por meio dos protocolos HTTP/HTTPS e FTP e verificar se os endereços da Web são maliciosos ou phishing;
6.4.13.2.12. 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;
6.4.13.2.13. Suporte ao gerenciamento de dispositivos conectados com limitações de tempo e usuário por meio do Samba Active Directory e do Microsoft AD;
6.4.13.2.14. Deve oferecer suporte à verificação de unidades removíveis quando elas estão conectadas a um computador;
6.4.13.2.15. Oferecer suporte à inspeção de tráfego de rede para atividades típicas de ataques de rede. Deve ser capaz de operar no modo somente notificação;
6.4.13.2.16. Suportar a verificação da reputação do objeto no banco de dados de reputação global;
6.4.13.2.17. Permitir que usuários não root gerenciem as funções básicas do aplicativo usando a GUI;
6.4.13.2.18. Oferecer suporte ao gerenciamento usando os seguintes métodos:
6.4.13.2.18.1. Na linha de comando usando os comandos de controle de aplicativos;
6.4.13.2.18.2. Via console de gerenciamento central (console baseado em MMC e console da web);
6.4.13.2.18.3. GUI local;
6.4.13.2.19. Deve suportar capacidade de detecção de comportamento. Deve ser capaz de operar no modo somente notificação;
6.4.13.2.20. Deve suportar o trabalho com o sistema de arquivos GlusterFS;
6.4.13.2.21. Deve suportar dispositivo de gerenciamento com a solução instalada via console de nuvem;
6.4.13.2.22. Deve suportar verificação da memória do kernel;
6.4.13.2.23. Oferecer suporte à verificação da integridade dos componentes do aplicativo;
6.4.13.2.24. Oferecer suporte aos recursos de controle de inicialização do aplicativo;
6.4.13.2.25. Deve ser capaz de obter informações sobre todos os arquivos de programas executáveis armazenados nos computadores;
6.4.13.2.26. Oferecer suporte à opção de gerenciamento baseado em perfil;

6.4.14. Requisitos para antivírus em ambientes virtualizados baseado em agente para datacenter;

6.4.14.1. A solução deve suportar a seguinte infraestrutura virtual:
6.4.14.1.1. Microsoft Windows Server 2012 R2 Hyper-V e posteriores;
6.4.14.1.2. Citrix 8.2 LTSR;
6.4.14.1.3. Hypervisor VMware ESXi 6.5 e posteriores;
6.4.14.1.4. Plataforma KVM: Hypervisor KVM com um dos seguintes sistemas operacionais:
6.4.14.1.4.1. Servidor Ubuntu 16.04 LTS ou posteriores;

6.4.14.1.4.2. Servidor Red Hat Enterprise Linux 7. 9;
6.4.14.1.4.3. CentOS 7.9;
6.4.14.1.5. Proxmox VE 6.3 e posteriores;
6.4.14.1.6. Hipervisor R-Virtualization 7.0.13;
6.4.14.1.7. HUAWEI FusionSphere;
6.4.14.1.8. HUAWEI FusionCompute CNA 8.0;
6.4.14.1.9. Hipervisor Nutanix AHV 5.19.1;
6.4.14.1.10. Lançamentos da plataforma OpenStack: Stein, Victoria, Wallaby ou Xena;
6.4.14.2. A solução deve suportar as seguintes soluções de virtualização:
6.4.14.2.1. Citrix Virtual Apps and Desktops 7 1912 LTSR;
6.4.14.2.2. Citrix XenApp e XenDesktop 7.15 LTSR;
6.4.14.2.3. Provisionamento Citrix 7 1912 LTSR;
6.4.14.2.4. Serviços de Provisionamento Citrix 7.15 LTSR;
6.4.14.2.5. VMware Horizon 8.2 (2103);
6.4.14.2.6. Volumes de aplicativos VMware (2103);
6.4.14.2.7. HUAWEI FusionAccess 8.0 e posterior;
6.4.14.3. Deve oferecer suporte aos seguintes sistemas operacionais:
6.4.14.3.1. Windows 11;
6.4.14.3.2. Windows 10; (32 / 64 bits);
6.4.14.3.3. Windows 8.1 Update 1 Professional/Enterprise (32/64 bits)
6.4.14.3.4. Windows 7 Pro / Enterprise SP1 (32/64 bits);
6.4.14.3.5. Windows Server 2019 Standard/ Datacenter (64 bits);
6.4.14.3.6. Windows Server 2016 Standard/ Datacenter (64 bits);
6.4.14.3.7. Windows Server 2012 e 2021 R2 Standard / Datacenter / Essentials (64 bits);
6.4.14.3.8. Windows Server 2008 R2 SP1 Standard / Enterprise / Datacenter (64 bits);
6.4.14.3.9. Debian GNU/Linux 10.3 (32/64 bits);
6.4.14.3.10. Debian GNU/Linux 9.8 (64 bits);
6.4.14.3.11. Debian GNU/Linux 8.11 (64 bits);
6.4.14.3.12. Debian GNU/Linux 8.11 i386 (32 bits);
6.4.14.3.13. Servidor Ubuntu 16.04 LTS e posteriores (64 bits);
6.4.14.3.14. CentOS 6.10 e posteriores (64 bits);
6.4.14.3.15. Red Hat Enterprise Linux Server 6.10 e posteriores (64 bits);
6.4.14.3.16. SUSE Linux Enterprise Server 15 (64 bits);
6.4.14.3.17. Oracle Linux 7.6 (64 bits);
6.4.14.4. Características:
6.4.14.4.1. Deve oferecer suporte ao monitoramento AntiMalware;
6.4.14.4.2. Deve ter um analisador heurístico para detectar e bloquear malware anteriormente desconhecido;
6.4.14.4.3. 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;
6.4.14.4.4. Se a máquina virtual segura principal estiver indisponível, o agente deve oferecer suporte à detecção automática e reconexão a uma máquina virtual segura em funcionamento, incluindo uma que esteja operando em um host diferente;
6.4.14.4.5. Técnicas de redundância, que permitem a reconexão do agente a qualquer máquina virtual segura dentro da infraestrutura sem qualquer (re)configuração manual;

6.4.14.4.6. A solução deve oferecer suporte à instalação remota do agente para Windows e Linux;
6.4.14.4.7. 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;
6.4.14.4.8. 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;
6.4.14.4.9. 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 ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.14.4.10. 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;
6.4.14.4.11. 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.
6.4.14.4.12. Oferecer suporte à proteção contra programas maliciosos ainda desconhecidos com base em seu comportamento;
6.4.14.4.13. 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;
6.4.14.4.14. 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;
6.4.14.4.15. 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);
6.4.14.4.16. 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;
6.4.14.4.17. 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;
6.4.14.4.18. 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;
6.4.14.4.19. Deve armazenar as atualizações do banco de dados AntiMalware em máquinas virtuais seguras;

6.4.14.4.20. Permitir que os administradores instalem e distribuam remotamente componentes de software AntiMalware em todas as máquinas virtuais protegidas sem usar ferramentas de terceiros;
6.4.14.4.21. Deve oferecer suporte à verificação programada de todas as máquinas virtuais;
6.4.14.4.22. A solução deve ter um único console de gerenciamento para todos os componentes de proteção;
6.4.14.4.23. A solução deve ter um único console de gerenciamento centralizado para ambientes virtuais e estações de trabalho físicas;

6.4.14.4.24. 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;
6.4.14.4.25. 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;
6.4.14.4.26. 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;
6.4.14.4.27. Deve fornecer informações detalhadas sobre eventos em máquinas virtuais e execução de tarefas de proteção;
6.4.14.4.28. Deve oferecer suporte à verificação de mensagens de e-mail recebidas e enviadas em busca de vírus e outros malwares;
6.4.14.4.29. Deve permitir que os administradores apliquem diferentes configurações de segurança para diferentes grupos de máquinas virtuais.
6.4.14.4.30. Deve oferecer suporte ao armazenamento de cópias de backup de arquivos excluídos.
6.4.14.4.31. Deve suportar a tecnologia VMware: vMotion, DRS;
6.4.14.4.32. Deve oferecer suporte para reversão de bancos de dados de antivírus;
6.4.14.4.33. Deve suportar um esquema de licenciamento de acordo com o número total de CPUs físicas de cada host/hipervisor;
6.4.14.4.34. Oferecer suporte à proteção de máquinas virtuais que executam os sistemas operacionais Windows e Linux;
6.4.14.4.35. Oferecer suporte ao console de administração unificado para implantação e gerenciamento eficientes de toda a infraestrutura de segurança de TI;
6.4.14.4.36. 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;
6.4.14.4.37. 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;
6.4.14.4.38. Deve ter proteção de rede integrada, que detecta e bloqueia ataques diretos à rede;
6.4.14.4.39. A solução deve oferecer suporte à proteção da Web integrada, que detecta e bloqueia URLs maliciosos;

6.4.14.4.40. Verifica todos os arquivos durante a verificação AntiMalware (mesmo arquivos maiores que 30 Mb);
6.4.14.4.41. A solução deve suportar o envio de notificações por e-mail e SMS;
6.4.14.4.42. Deve ter uma política de segurança para gerenciar todos os módulos de proteção;
6.4.14.4.43. Deve ser compatível com NSX Security Tags;
6.4.14.4.44. Deve oferecer suporte à proteção de pastas compartilhadas contra criptografia remota;
6.4.14.4.45. Deve oferecer suporte para ativação usando um código de ativação fornecido na assinatura;
6.4.14.4.46. 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;
6.4.14.4.47. 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;
6.4.14.4.48. Deve oferecer suporte para o sistema de arquivos GlusterFS em máquinas virtuais que tenham o agente para Linux instalado;
6.4.14.4.49. A solução deve permitir o uso do aplicativo no modo multilocação;
6.4.14.4.50. Deve fornecer a capacidade de automatizar a implantação e o uso do aplicativo no modo multilocação usando a API REST;
6.4.14.4.51. 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;
6.4.14.4.52. O controle de aplicativos para Windows Servers deve ter lógica de lista branca e lista negra;
6.4.14.4.53. 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;
6.4.14.4.54. A solução deve fornecer recursos de integração com o serviço gerenciado de detecção e resposta do mesmo fornecedor;

6.4.15. Requisitos para antivírus em ambientes virtualizados sem agentes para datacenter;

6.4.15.1. A solução deve suportar a seguinte infraestrutura virtual:
6.4.15.1.1. VMware vSphere versões 8.0 e 7.0;
6.4.15.1.2. VMware ESXi 6.5 Atualização 3 ou posterior;
6.4.15.1.3. VMware vCenter Server 6.5 Atualização 3 ou posterior;
6.4.15.2. VMware NSX Manager de um dos seguintes tipos:
6.4.15.2.1. NSX-V Manager do pacote VMware NSX Data Center para vSphere 6.4.10;
6.4.15.2.2. NSX-T Manager do VMware NSX 4.0.1.1, VMware NSX 4.0.0.1, VMware NSXT 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;
6.4.15.2.3. 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;
6.4.15.2.4. VMware vCloud Director 9.7.0.3 para provedores de serviços;
6.4.15.2.5. VMware vCloud Diretor versões 10.4, 10.3.3.2, 10.3.2.1, 10.3.0, 10.1.2;

6.4.15.3. A solução deve oferecer suporte aos seguintes sistemas operacionais:
6.4.15.3.1. Windows 10
6.4.15.3.2. Windows 8.1;
6.4.15.3.3. Windows 8;
6.4.15.3.4. Windows 7 SP1;
6.4.15.3.5. Windows Server 2019;
6.4.15.3.6. Windows Server 2016;
6.4.15.3.7. Windows Server 2012 e 2012 R2 sem suporte a ReFS;
6.4.15.3.8. Windows Server 2008 R2 SP1;
6.4.15.3.9. Ubuntu Server 14.04 GA e posteriores (64 bits);
6.4.15.3.10. Red Hat Enterprise Linux Server 7.0 GA e posteriores (64 bits);
6.4.15.3.11. SUSE Linux Enterprise Server 12 GA (64 bits);
6.4.15.3.12. CentOS 7.0 GA e posteriores (64 bits);
6.4.15.4. Características:
6.4.15.4.1. Oferecer suporte à proteção contra malware em tempo real e durante a verificação agendada sem instalar um agente antivírus nas máquinas virtuais convidadas;
6.4.15.4.2. 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;
6.4.15.4.3. 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;
6.4.15.4.4. Suportar atualizações centralizadas na máquina de proteção especializada sem a necessidade de distribuir atualizações para cada máquina convidada;
6.4.15.4.5. Suporte à verificação sob demanda (ou manual) de máquinas virtuais selecionadas;
6.4.15.4.6. Oferecer suporte à verificação de arquivos, pastas ou de todo o sistema selecionados;
6.4.15.4.7. Suporte à verificação programada de todas as máquinas virtuais;
6.4.15.4.8. Fornecer a capacidade de implantar uma solução sem reinicialização do hipervisor ou modo de manutenção;
6.4.15.4.9. A solução não deve exigir uma nova verificação dos arquivos;
6.4.15.4.10. Deve impedir a nova verificação do mesmo objeto em diferentes máquinas convidadas em um único host;
6.4.15.4.11. Deve suportar bloqueio, neutralização e remoção de malware, notificação de administradores;
6.4.15.4.12. Deve permitir que os administradores vejam a estrutura de administração física e lógica conforme ela é apresentada no VMware vCenter;
6.4.15.4.13. Deve fornecer ao administrador informações detalhadas sobre eventos em máquinas virtuais e a implementação de tarefas;
6.4.15.4.14. Deve permitir que os administradores apliquem diferentes configurações de segurança para diferentes grupos de máquinas virtuais;
6.4.15.4.15. 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;
6.4.15.4.16. Permitir que os administradores exportem/importem uma lista de exceções;
6.4.15.4.17. Deve incluir a lista de exceções frequentes compiladas de acordo com as recomendações da Microsoft;
6.4.15.4.18. Deve permitir que os administradores verifiquem as unidades de rede conectadas à máquina virtual protegida, se necessário;
6.4.15.4.19. Permitir que os administradores excluam as unidades de rede da proteção;
6.4.15.4.20. Deve oferecer suporte para VMware vMotion e DRS;
6.4.15.4.21. Oferecer suporte ao armazenamento de cópias de backup de arquivos excluídos;
6.4.15.4.22. Deve suportar um esquema de licenciamento de acordo com o número total de CPUs físicas de cada host/hipervisor;
6.4.15.4.23. 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;
6.4.15.4.24. A solução deve oferecer suporte para ativação usando um código de ativação fornecido na assinatura;
6.4.15.4.25. Deve fornecer informações sobre o número de objetos verificados;
6.4.15.4.26. Deve fornecer informações sobre os detalhes do banco de dados de antivírus;

6.4.15.4.27. Deve oferecer suporte à verificação de certificados SSL para comunicação entre o mecanismo AntiMalware, o servidor de gerenciamento e os componentes da infraestrutura VMware;
6.4.15.4.28. Deve permitir que os administradores importem ou exportem a lista de exclusões de verificação e proteção em tarefas de verificação e perfis de proteção;
6.4.15.4.29. Deve permitir que os administradores protejam as máquinas virtuais que executam os sistemas operacionais Windows e Linux;
6.4.15.4.30. 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;
6.4.15.4.31. Deve permitir que os administradores especifiquem diferentes ações para ameaças encontradas em máquinas virtuais ligadas e desligadas;
6.4.15.4.32. Oferecer suporte ao modo multilocação - uma infraestrutura gerenciada por um VMware vCloud Director;
6.4.15.4.33. A solução deve ter a capacidade de verificar a reputação dos recursos da Web em relação a um banco de dados global de ameaças;
6.4.15.4.34. 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;
6.4.15.4.35. Deve ser capaz de desbloquear ataques de rede bloqueados incorretamente (Falso Positivo) sem demora;
6.4.15.4.36. Deve incluir a capacidade de verificar endereços da Web em um banco de dados global de endereços de phishing;
6.4.15.4.37. Deve ser capaz de restringir o acesso para configuração com base em contas

de usuário;
6.4.15.4.38. Deve ser capaz de verificar máquinas virtuais Linux desligadas com os seguintes sistemas de arquivos: EXT2, EXT3, EXT4, XFS, BTRFS;
6.4.15.4.39. Deve ser capaz de digitalizar modelos de máquina virtual;
6.4.15.4.40. 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;
6.4.15.4.41. A solução deve suportar o serviço SNMP. Por exemplo: Receber informações sobre o estado atual do componente IDS/IPS;
6.4.15.4.42. A solução deve suportar ambiente de grande escala;

ITEM 03 - SOFTWARE DE SEGURANÇA E ANTIVÍRUS PARA AMBIENTES VIRTUALIZADOS EM CLOUD

6.4.16. Requerimentos para gerenciamento, administração e relatórios centralizados

6.4.16.1. Permitir a instalação de software AntiMalware a partir de um único pacote de distribuição;
6.4.16.2. Deve ter perfis de instalação personalizáveis dependendo do número de nós protegidos;
6.4.16.3. Suportar endereços IPv6.
6.4.16.4. Suportar verificação em duas etapas (autenticação);
6.4.16.5. Deve ter capacidade de ler informações do AD para obter dados sobre contas de computadores na organização;
6.4.16.6. Deverá incluir uma consola web incorporada para a gestão dos endpoints, que não deverá necessitar de qualquer instalação adicional;
6.4.16.7. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos de tela sensível ao toque;
6.4.16.8. Deve distribuir automaticamente as contas de computador por grupo de gerenciamento se novos computadores aparecerem na rede;
6.4.16.9. 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 AD;
6.4.16.10. Deverá prever a instalação, atualização e remoção centralizada de software AntiMalware, bem como configuração, administração e visualização centralizada de relatórios e informações estatísticas sobre o seu funcionamento;
6.4.16.11. Deverá contemplar a remoção centralizada (manual e automática) de aplicativos incompatíveis do centro de administração;
6.4.16.12. Deverá 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;
6.4.16.13. Deverá permitir a instalação remota de software AntiMalware com as bases de dados AntiMalware mais recentes;
6.4.16.14. Deve permitir a atualização automática do software AntiMalware e das bases

de dados AntiMalware;
6.4.16.15. Deve possibilitar o gerenciamento de um componente que proíba a instalação e /ou execução de programas;
6.4.16.16. Deve oferecer suporte à integração de API nativa com o Microsoft Azure e Google Cloud Platform;
6.4.16.17. Deve oferecer suporte à integração nativa da API com o ambiente de nuvem Amazon AWS, que inclui autenticação e localização de dispositivos usando a API AWS
6.4.16.18. Deve oferecer suporte à instalação remota de proteção usando API na AWS;
6.4.16.19. O servidor de gerenciamento centralizado da solução exibe recursos específicos da AWS (propriedades do dispositivo cliente, hierarquia de grupos de administração, Diretório AWS, assistente de configuração de proteção de segmento de nuvem e sondagem de segmento de nuvem) em sua interface;
6.4.16.20. Deve oferecer suporte a esquemas de licenciamento BYOL e PAYGo para proteção de nuvem pública;
6.4.16.21. Deve possibilitar o gerenciamento de um componente controlando o trabalho com dispositivos de E/S externos;
6.4.16.22. Deve possibilitar o gerenciamento de um componente que controla a atividade do usuário na internet;
6.4.16.23. 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;
6.4.16.24. 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;
6.4.16.25. 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;
6.4.16.26. 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;
6.4.16.27. Deve dar acesso aos serviços de nuvem do fornecedor de segurança AntiMalware por meio do servidor de administração;
6.4.16.28. Deve incluir a distribuição automática de licenças nos computadores clientes;
6.4.16.29. Deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários;
6.4.16.30. Deve ter um mecanismo de notificação para informar os usuários sobre eventos no software AntiMalware instalado e nas configurações, e para distribuir notificações sobre eventos via e-mail;
6.4.16.31. Permitir a instalação centralizada de aplicativos de terceiros em todos ou em alguns computadores;
6.4.16.32. 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.
6.4.16.33. Capacidade de especificar qualquer computador da organização como um

centro de encaminhamento de eventos do agente AntiMalware 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;
6.4.16.34. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software AntiMalware, e dados sobre o inventário de hardware e software, licenciamento, etc.;
6.4.16.35. Deve ser capaz de exportar relatórios para arquivos PDF e XML;
6.4.16.36. Deve fornecer a administração centralizada de armazenamentos de backup e quarentena em todos os recursos de rede onde o software AntiMalware está instalado;
6.4.16.37. Deve prever a criação de contas internas para autenticar administradores no servidor de administração;
6.4.16.38. Deve prever a criação de uma cópia de backup do sistema de administração com o auxílio de ferramentas integradas do sistema de administração;
6.4.16.39. Deve oferecer suporte ao Windows Failover Cluster ou compor com outra solução de alta disponibilidade;
6.4.16.40. Deve ter um recurso de cluster integrado;
6.4.16.41. Deve incluir alguma forma de sistema para controlar epidemias de vírus;
6.4.16.42. 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;
6.4.16.43. O servidor de gerenciamento da solução deve incluir funções de segurança pré-definidas para Auditor, Supervisor e Agente de Segurança;
6.4.16.44. Capacidade de gerenciar dispositivos móveis por meio de comandos remotos;
6.4.16.45. Capacidade de excluir as atualizações baixadas;
6.4.16.46. Deve gerar atualizações do Servidor de Administração de Gerenciamento a partir da interface do aplicativo;
6.4.16.47. Deve permitir a seleção de um agente de atualização para computadores clientes com base em uma análise de rede;
6.4.16.48. O servidor de gerenciamento da solução 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;
6.4.16.49. O servidor de gerenciamento da solução 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:
6.4.16.49.1. Status do dispositivo;
6.4.16.49.2. Tag;
6.4.16.49.3. Diretório ativo;
6.4.16.49.4. Proprietários de dispositivos;
6.4.16.49.5. Hardware;
6.4.16.50. Suportar os seguintes canais de entrega de notificação:
6.4.16.50.1. E-mail;
6.4.16.50.2. Syslog;
6.4.16.51. 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;

6.4.16.52. Capacidade de realizar inventário em scripts e arquivos. arquivos dll;
6.4.16.53. Deve ter a capacidade de etiquetar/marcar computadores com base em:
6.4.16.53.1. Atributos de rede;
6.4.16.53.2. Nome;
6.4.16.53.3. Domínio e/ou Sufixo de Domínio;
6.4.16.53.4. IP;
6.4.16.53.5. Endereço IP para o servidor de gerenciamento;
6.4.16.53.6. Localização no Active Directory;
6.4.16.53.7. Unidade organizacional;
6.4.16.53.8. Grupo;
6.4.16.53.9. Sistema operacional;
6.4.16.53.10. Tipo e versão;
6.4.16.53.11. Arquitetura;
6.4.16.53.12. Número do pacote de serviço;
6.4.16.53.13. Arquitetura virtual;
6.4.16.53.14. Registro de aplicativos;
6.4.16.53.15. Nome da Aplicação;
6.4.16.53.16. Versão do aplicativo;
6.4.16.53.17. Fabricante;
6.4.16.54. A solução 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;

6.4.16.55. Deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectando pela internet/rede pública;
6.4.16.56. 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 definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis;
6.4.16.57. Ter um painel personalizável gerando e exibindo estatísticas em tempo real para endpoints;
6.4.16.58. Deve permitir que o administrador personalize os relatórios;
6.4.16.59. Deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado;
6.4.16.60. Deve permitir que o administrador estabeleça um período após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados são excluídos automaticamente do servidor;
6.4.16.61. A solução deve permitir ao administrador criar categorias/grupos de aplicação com base em:
6.4.16.61.1. Nome da Aplicação;
6.4.16.61.2. Caminho do Aplicativo;
6.4.16.61.3. Metadados do aplicativo;
6.4.16.61.4. Aplicativo certificado digital;
6.4.16.61.5. Categorias de aplicativos pré-definidas pelo fornecedor;

6.4.16.61.6. SHA;
6.4.16.62. Computadores de referência para permitir/negar sua execução em endpoints;
6.4.16.63. Permitir que o administrador defina diferentes condições de alteração de status para grupos de endpoints no servidor de gerenciamento;
6.4.16.64. Permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento;
6.4.16.65. Deve ter um recurso/módulo embutido para coletar remotamente os dados necessários para solução de problemas dos endpoints, sem exigir acesso físico;
6.4.16.66. 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;
6.4.16.67. 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;
6.4.16.68. Deve possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:
6.4.16.68.1. Estruturas de domínios e grupos de trabalho do Windows;
6.4.16.68.2. Estruturas de grupos do AD;
6.4.16.68.3. Conteúdo de um arquivo de texto criado pelo administrador manualmente;
6.4.16.68.4. Ambiente AWS;
6.4.16.69. A solução 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;
6.4.16.70. As informações sobre o equipamento devem ser atualizadas após cada nova pesquisa de rede. A lista de equipamentos detectados deve abranger o seguinte:
6.4.16.70.1. Dispositivos;
6.4.16.70.2. Dispositivos móveis;
6.4.16.70.3. Dispositivos de rede;
6.4.16.70.4. Dispositivos virtuais;
6.4.16.70.5. Componentes OEM;
6.4.16.70.6. Periféricos de computador;
6.4.16.70.7. Dispositivos conectados;
6.4.16.70.8. Telefones VoIP;
6.4.16.70.9. Repositórios de rede;
6.4.16.71. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede;
6.4.16.72. A funcionalidade 'Device is Write Off' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos;
6.4.16.73. A solução deve incorporar um único agente de distribuição/retransmissão para dar suporte a pelo menos 10.000 endpoints para a entrega de proteção, atualizações, patches e pacotes de instalação para sites remotos;
6.4.16.74. 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;

6.4.16.75. Deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização;
6.4.16.76. Deve suportar OPEN API e incluir diretrizes para integração com sistemas externos de terceiros;
6.4.16.77. A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem a necessidade de acesso físico ao computador;
6.4.16.78. A solução proposta deve incluir Controle de Acesso Baseado em Função (RBAC) com funções predefinidas personalizáveis;
6.4.16.79. O servidor de gerenciamento primário/pai da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem;
6.4.16.80. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou;
6.4.16.81. O relatório da solução 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;
6.4.16.82. O servidor de gerenciamento principal deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade etc., dos terminais gerenciados dos servidores de gerenciamento secundário;
6.4.16.83. 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;
6.4.16.84. A solução deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional;
6.4.16.85. Deve permitir uma migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor;
6.4.16.86. Deve incluir a opção de integração SIEM – Syslog;
6.4.16.87. Deve incluir suporte para implantação baseada em nuvem por meio de:
6.4.16.87.1. Amazon Web Services;
6.4.16.87.2. Microsoft Azure;
6.4.16.88. Deve fornecer mecanismos de atualização de banco de dados AntiMalware, incluindo:
6.4.16.88.1. Múltiplas formas de atualização, incluindo canais de comunicação globais sobre o protocolo HTTPS, recurso compartilhado na rede local e mídia removível;
6.4.16.88.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica;
6.4.16.89. A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos;
6.4.17. Requisitos para antivírus em ambientes virtualizados baseado em agente para Windows;
6.4.17.1. Oferecer suporte aos seguintes sistemas operacionais:
6.4.17.1.1. Windows 11 21H2 Pro/Enterprise/Education;
6.4.17.1.2. Windows 10 Desktop Pro 19H1/19H2/20H1/20H2/21H1 (32 / 64-bit);
6.4.17.1.3. Windows 10 Enterprise 2016 LTSC/2019 LTSC/19H1/19H2/20H1/20H2/21H1 (32 / 64-bit);
6.4.17.1.4. Windows 8.1 Update 1 Professional/Enterprise (32 / 64-bit);
6.4.17.1.5. Windows 7 Professional/Enterprise SP1 (32/64-bit);

6.4.17.1.6. Windows Server 2022 Standard/ Datacenter /Essentials (Desktop experience /Core);
6.4.17.1.7. Windows Server 2019 Standard/ Datacenter (Desktop experience/Core);
6.4.17.1.8. Windows Server 2016 Standard/ Datacenter (Desktop experience/Core);
6.4.17.1.9. Windows Server 2012 R2 Standard/ Datacenter /Essentials (Desktop experience/Core);
6.4.17.1.10. Windows Server 2012 Standard/ Datacenter /Essentials (Desktop experience /Core);
6.4.17.1.11. Windows Server 2008 R2 SP1 Standard/Enterprise/ Datacenter (Desktop experience/Core);
6.4.17.2. Características:
6.4.17.2.1. Oferecer suporte à verificação de objetos quando eles são acessados;
6.4.17.2.2. Suporte a verificações dos seguintes objetos:
6.4.17.2.2.1. Arquivos;
6.4.17.2.2.2. Fluxos alternativos do sistema de arquivos (fluxos NTFS);
6.4.17.2.2.3. Registro de inicialização e setores de inicialização em discos rígidos locais e unidades removíveis;
6.4.17.2.3. Suportar varredura sob demanda para executar 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;
6.4.17.2.4. 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;
6.4.17.2.5. Deve oferecer suporte a pastas compartilhadas de proteção em dispositivos contra criptografia maliciosa, bloqueando hosts que mostram atividade maliciosa;
6.4.17.2.6. Deve controlar a execução de scripts usando tecnologias de script do Microsoft Windows;
6.4.17.2.7. 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;
6.4.17.2.8. Deve verificar o tráfego de rede em busca de atividades típicas de ataques de rede e bloquear a atividade de rede do computador atacante;
6.4.17.2.9. 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;
6.4.17.2.10. 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;
6.4.17.2.11. Deve colocar em quarentena os objetos provavelmente infectados, movendoos 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;
6.4.17.2.12. Armazenar cópias criptografadas de objetos classificados como infectados no backup antes de desinfetá-los ou excluí-los;
6.4.17.2.13. Oferecer suporte a notificações do usuário;

6.4.17.2.14. Oferecer suporte à importação e exportação de configurações;
6.4.17.2.15. 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;
6.4.17.2.16. Deve oferecer suporte à proteção de memória contra explorações;
6.4.17.2.17. Deve suportar dispositivo de gerenciamento com a solução instalada via console de nuvem;
6.4.17.2.18. Fornecer integração com os mesmos fornecedores de Detecção de Endpoint e Resposta “EDR”, para busca ativa de ameaças e automação de resposta a incidentes;

6.4.18. Requisitos para antivírus em ambientes virtualizados baseado em agente para Linux;

6.4.18.1. A solução deve oferecer suporte aos seguintes sistemas operacionais:
6.4.18.1.1. CentOS 7.3 e posteriores (64-bit);
6.4.18.1.2. Debian GNU/Linux 9.4 e posteriores (32/64-bit);
6.4.18.1.3. Oracle Linux 7.3 e posteriores (64-bit);
6.4.18.1.4. Red Hat Enterprise Linux Server 7.3 e posteriores (64-bit);
6.4.18.1.5. SUSE Linux Enterprise Server 15 SP2 (64-bit);
6.4.18.1.6. Ubuntu 18.04 LTS e posteriores (64-bit);
6.4.18.2. Características:
6.4.18.2.1. 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;
6.4.18.2.2. Oferecer suporte a varredura de objetos do sistema de arquivos em tempo real e sob demanda;
6.4.18.2.3. Deve oferecer suporte a digitalização de objetos de inicialização, setores de inicialização, processo e memória do kernel;
6.4.18.2.4. Suportar neutralizar ameaças detectadas em arquivos e escolher automaticamente qual ação executar para neutralizar a ameaça;
6.4.18.2.5. Oferecer suporte ao armazenamento de cópias de backup de arquivos antes da desinfecção ou exclusão e restauração de arquivos de cópias de backup;
6.4.18.2.6. Oferecer suporte à notificação do administrador sobre eventos ocorridos durante a operação;
6.4.18.2.7. 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;
6.4.18.2.8. Suporte à adição de chaves, bem como à ativação usando códigos de ativação;
6.4.18.2.9. Suporte ao gerenciamento de um firewall do sistema operacional;
6.4.18.2.10. Suporte à proteção de seus arquivos nos diretórios locais com acesso à rede por protocolos SMB/NFS contra criptografia maliciosa remota;
6.4.18.2.11. Suporte à verificação de tráfego por meio dos protocolos HTTP/HTTPS e FTP e verificar se os endereços da Web são maliciosos ou phishing;
6.4.18.2.12. 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;
6.4.18.2.13. Suporte ao gerenciamento de dispositivos conectados com limitações de tempo e usuário por meio do Samba Active Directory e do Microsoft AD;
6.4.18.2.14. Deve oferecer suporte à verificação de unidades removíveis quando elas estão conectadas a um computador;
6.4.18.2.15. Oferecer suporte à inspeção de tráfego de rede para atividades típicas de ataques de rede. Deve ser capaz de operar no modo somente notificação;
6.4.18.2.16. Suportar a verificação da reputação do objeto no banco de dados de reputação global;
6.4.18.2.17. Permitir que usuários não root gerenciem as funções básicas do aplicativo usando a GUI;
6.4.18.2.18. Oferecer suporte ao gerenciamento usando os seguintes métodos:
6.4.18.2.18.1. Na linha de comando usando os comandos de controle de aplicativos;
6.4.18.2.18.2. Via console de gerenciamento central (console baseado em MMC e console da web);
6.4.18.2.18.3. GUI local;
6.4.18.2.19. Deve suportar capacidade de detecção de comportamento. Deve ser capaz de operar no modo somente notificação;
6.4.18.2.20. Deve suportar o trabalho com o sistema de arquivos GlusterFS;
6.4.18.2.21. Deve suportar dispositivo de gerenciamento com a solução instalada via console de nuvem;
6.4.18.2.22. Deve suportar verificação da memória do kernel;
6.4.18.2.23. Oferecer suporte à verificação da integridade dos componentes do aplicativo;
6.4.18.2.24. Oferecer suporte aos recursos de controle de inicialização do aplicativo;
6.4.18.2.25. Deve ser capaz de obter informações sobre todos os arquivos de programas executáveis armazenados nos computadores;
6.4.18.2.26. Oferecer suporte à opção de gerenciamento baseado em perfil;

6.4.19. Requisitos para antivírus em ambientes virtualizados baseado em agente para datacenter;

6.4.19.1. A solução deve suportar a seguinte infraestrutura virtual:
6.4.19.1.1. Microsoft Windows Server 2012 R2 Hyper-V e posteriores;
6.4.19.1.2. Citrix 8.2 LTSR;
6.4.19.1.3. Hypervisor VMware ESXi 6.5 e posteriores;
6.4.19.1.4. Plataforma KVM: Hypervisor KVM com um dos seguintes sistemas operacionais:
6.4.19.1.4.1. Servidor Ubuntu 16.04 LTS ou posteriores;
6.4.19.1.4.2. Servidor Red Hat Enterprise Linux 7. 9;
6.4.19.1.4.3. CentOS 7.9;
6.4.19.1.5. Proxmox VE 6.3 e posteriores;
6.4.19.1.6. Hipervisor R-Virtualization 7.0.13;
6.4.19.1.7. HUAWEI FusionSphere;
6.4.19.1.8. HUAWEI FusionCompute CNA 8.0;

6.4.19.1.9. Hipervisor Nutanix AHV 5.19.1;
6.4.19.1.10. Lançamentos da plataforma OpenStack: Stein, Victoria, Wallaby ou Xena;
6.4.19.2. A solução deve suportar as seguintes soluções de virtualização:
6.4.19.2.1. Citrix Virtual Apps and Desktops 7 1912 LTSR;
6.4.19.2.2. Citrix XenApp e XenDesktop 7.15 LTSR;
6.4.19.2.3. Provisionamento Citrix 7 1912 LTSR;
6.4.19.2.4. Serviços de Provisionamento Citrix 7.15 LTSR;
6.4.19.2.5. VMware Horizon 8.2 (2103);
6.4.19.2.6. Volumes de aplicativos VMware (2103);
6.4.19.2.7. HUAWEI FusionAccess 8.0 e posterior;
6.4.19.3. Deve oferecer suporte aos seguintes sistemas operacionais:
6.4.19.3.1. Windows 11;
6.4.19.3.2. Windows 10; (32 / 64 bits);
6.4.19.3.3. Windows 8.1 Update 1 Professional/Enterprise (32/64 bits)
6.4.19.3.4. Windows 7 Pro / Enterprise SP1 (32/64 bits);
6.4.19.3.5. Windows Server 2019 Standard/ Datacenter (64 bits);
6.4.19.3.6. Windows Server 2016 Standard/ Datacenter (64 bits);
6.4.19.3.7. Windows Server 2012 e 2021 R2 Standard / Datacenter / Essentials (64 bits);
6.4.19.3.8. Windows Server 2008 R2 SP1 Standard / Enterprise / Datacenter (64 bits);
6.4.19.3.9. Debian GNU/Linux 10.3 (32/64 bits);
6.4.19.3.10. Debian GNU/Linux 9.8 (64 bits);
6.4.19.3.11. Debian GNU/Linux 8.11 (64 bits);
6.4.19.3.12. Debian GNU/Linux 8.11 i386 (32 bits);
6.4.19.3.13. Servidor Ubuntu 16.04 LTS e posteriores (64 bits);
6.4.19.3.14. CentOS 6.10 e posteriores (64 bits);
6.4.19.3.15. Red Hat Enterprise Linux Server 6.10 e posteriores (64 bits);
6.4.19.3.16. SUSE Linux Enterprise Server 15 (64 bits);
6.4.19.3.17. Oracle Linux 7.6 (64 bits);
6.4.19.4. Características:
6.4.19.4.1. Deve oferecer suporte ao monitoramento AntiMalware;
6.4.19.4.2. Deve ter um analisador heurístico para detectar e bloquear malware anteriormente desconhecido;
6.4.19.4.3. 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;
6.4.19.4.4. Se a máquina virtual segura principal estiver indisponível, o agente deve oferecer suporte à detecção automática e reconexão a uma máquina virtual segura em funcionamento, incluindo uma que esteja operando em um host diferente;

6.4.19.4.5. Técnicas de redundância, que permitem a reconexão do agente a qualquer máquina virtual segura dentro da infraestrutura sem qualquer (re)configuração manual;
6.4.19.4.6. A solução deve oferecer suporte à instalação remota do agente para Windows e Linux;
6.4.19.4.7. 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;
6.4.19.4.8. 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;
6.4.19.4.9. 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, ou compor com ferramenta do mesmo fabricante que tenha capacidade similar;
6.4.19.4.10. 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;
6.4.19.4.11. 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.
6.4.19.4.12. Oferecer suporte à proteção contra programas maliciosos ainda desconhecidos com base em seu comportamento;
6.4.19.4.13. 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;
6.4.19.4.14. 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;
6.4.19.4.15. 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);
6.4.19.4.16. 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;
6.4.19.4.17. 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;
6.4.19.4.18. 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;
6.4.19.4.19. Deve armazenar as atualizações do banco de dados AntiMalware em máquinas virtuais seguras;
6.4.19.4.20. Permitir que os administradores instalem e distribuam remotamente componentes de software AntiMalware em todas as máquinas virtuais protegidas sem usar ferramentas de terceiros;
6.4.19.4.21. Deve oferecer suporte à verificação programada de todas as máquinas virtuais;
6.4.19.4.22. A solução deve ter um único console de gerenciamento para todos os

componentes de proteção;
6.4.19.4.23. A solução deve ter um único console de gerenciamento centralizado para ambientes virtuais e estações de trabalho físicas;
6.4.19.4.24. 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;
6.4.19.4.25. 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;
6.4.19.4.26. 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;
6.4.19.4.27. Deve fornecer informações detalhadas sobre eventos em máquinas virtuais e execução de tarefas de proteção;
6.4.19.4.28. Deve oferecer suporte à verificação de mensagens de e-mail recebidas e enviadas em busca de vírus e outros malwares;
6.4.19.4.29. Deve permitir que os administradores apliquem diferentes configurações de segurança para diferentes grupos de máquinas virtuais.
6.4.19.4.30. Deve oferecer suporte ao armazenamento de cópias de backup de arquivos excluídos.
6.4.19.4.31. Deve suportar a tecnologia VMware: vMotion, DRS;
6.4.19.4.32. Deve oferecer suporte para reversão de bancos de dados de antivírus;
6.4.19.4.33. Deve suportar um esquema de licenciamento de acordo com o número total de VM (virtual machines);
6.4.19.4.34. Oferecer suporte à proteção de máquinas virtuais que executam os sistemas operacionais Windows e Linux;

6.4.19.4.35. Oferecer suporte ao console de administração unificado para implantação e gerenciamento eficientes de toda a infraestrutura de segurança de TI;
6.4.19.4.36. 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;
6.4.19.4.37. 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;
6.4.19.4.38. Deve ter proteção de rede integrada, que detecta e bloqueia ataques diretos à rede;
6.4.19.4.39. A solução deve oferecer suporte à proteção da Web integrada, que detecta e bloqueia URLs maliciosos;
6.4.19.4.40. Verifica todos os arquivos durante a verificação AntiMalware (mesmo arquivos maiores que 30 Mb);
6.4.19.4.41. A solução deve suportar o envio de notificações por e-mail e SMS;
6.4.19.4.42. Deve ter uma política de segurança para gerenciar todos os módulos de proteção;

6.4.19.4.43. Deve ser compatível com NSX Security Tags;
6.4.19.4.44. Deve oferecer suporte à proteção de pastas compartilhadas contra criptografia remota;
6.4.19.4.45. Deve oferecer suporte para ativação usando um código de ativação fornecido na assinatura;
6.4.19.4.46. 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;
6.4.19.4.47. 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;
6.4.19.4.48. Deve oferecer suporte para o sistema de arquivos GlusterFS em máquinas virtuais que tenham o agente para Linux instalado;
6.4.19.4.49. A solução deve permitir o uso do aplicativo no modo multilocação;
6.4.19.4.50. Deve fornecer a capacidade de automatizar a implantação e o uso do aplicativo no modo multilocação usando a API REST;
6.4.19.4.51. 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;
6.4.19.4.52. O controle de aplicativos para Windows Servers deve ter lógica de lista branca e lista negra;
6.4.19.4.53. 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;
6.4.19.4.54. A solução deve fornecer recursos de integração com o serviço gerenciado de detecção e resposta do mesmo fornecedor;

ITEM 04 – SOFTWARE DE COMPLEMENTO DE DETECÇÃO E RESPOSTA PARA OS ITENS 02 E 03
6.4.20. Deverá ser compatível com os seguintes sistemas operacionais:

6.4.20.1. Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;
6.4.20.2. Microsoft Windows 8 Professional/Enterprise;
6.4.20.3. Microsoft Windows 8.1 Professional / Enterprise;
6.4.20.4. Microsoft Windows 10 Pro / Enterprise / Home / Education;
6.4.20.5. Microsoft Windows 11 Pro / Enterprise / Home / Education;
6.4.20.6. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;
6.4.20.7. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;
6.4.20.8. Windows Server 2016 Essentials / Standard / Datacenter;
6.4.20.9. Windows Server 2019 Essentials / Standard / Datacenter;
6.4.20.10. Windows Server 2022.

6.4.21. Das características do módulo de EDR:

6.4.21.1. As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;
6.4.21.2. A solução deve oferecer módulo focado em capacidades de EDR “Endpoint

Detection and Response", incluindo no mínimo as seguintes capacidades:
6.4.21.2.1. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;
6.4.21.2.2. Deve fornecer graficamente a visualização da cadeia do ataque;
6.4.21.2.3. Deve possuir a capacidade de varredura, identificando a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).
6.4.21.3. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:
6.4.21.3.1. Isolar o host;
6.4.21.3.2. Iniciar uma varredura nas áreas críticas;
6.4.21.3.3. Quarentenar o objeto;
6.4.21.4. A solução deve criar um relatório detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:
6.4.21.4.1. Visibilidade das detecções provenientes de endpoint;
6.4.21.4.2. Processos;
6.4.21.4.3. Conexões remotas;
6.4.21.4.4. Alterações de registros;
6.4.21.4.5. Objetos baixados
6.4.21.4.6. Capacidade de integração com a solução de SandBox cloud do fabricante;
6.4.21.5. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador;
6.4.21.6. Deverá possuir informações de assinaturas digitais da ameaça;
6.4.21.7. Deve ser capaz de trazer informações do arquivo sobre sua geolocalização;
6.4.21.8. Possibilidade de informar quando o arquivo foi detectado pela base de conhecimento;
6.4.21.9. Trazer a identificação de comportamento e/ou descrição sobre o arquivo;
6.4.21.10. A solução deve oferecer no mínimo as seguintes opções de resposta:
6.4.21.10.1. Prevenir a execução de um arquivo;
6.4.21.10.2. Quarentenar um arquivo;
6.4.21.10.3. Iniciar uma varredura por IoC;
6.4.21.10.4. Parar um processo;
6.4.21.10.5. Executar um processo;
6.4.21.11. Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:
6.4.21.11.1. A opção de isolamento deve estar disponível junto a visualização do incidente;
6.4.21.11.2. Deverá ser possível remover a máquina do isolamento a partir do incidente;
6.4.21.11.3. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;
6.4.21.12. Na análise do incidente a ferramenta deverá apresentar recomendações de ações necessárias para executar para remediar o incidente;
6.4.21.13. A recomendação deve ser guiada juntamente com guias das opções selecionadas pelo analista, apresentando pop-up guiando as ações.
6.4.21.14. Deverá oferecer informações de inteligência de ameaças do próprio fabricante;

6.4.21.15. Deverá possuir detecção baseada em sandbox do tipo cloud;
6.4.21.16. Deverá suportar IoC de terceiros em formatos OpenIOC.

ITEM 05 – SOFTWARE DE DETECÇÃO E RESPOSTA GERENCIADO

6.4.22. Do monitoramento, identificação e investigação dos eventos de segurança cibernética

6.4.22.1. O serviço de monitoramento deverá utilizar informações extraídas de registros gerados pelos sistemas monitorados;
6.4.22.2. Deverá ser instalado agentes específicos nos servidores e desktops, objetivando coletar informações mais detalhadas para o serviço de monitoramento, desde que seja plenamente compatível com o sistema onde será instalado e não afete o desempenho dos serviços;
6.4.22.3. A análise das informações correlacionadas deve ser realizada com auxílio de bases globais de inteligência cibernética em conjunto com a expertise dos profissionais do fabricante, com vistas a reduzir ao máximo os falsos positivos;
6.4.22.4. É obrigatório que a comunicação entre equipamentos e soluções do fabricante instalados nos dispositivos e qualquer infraestrutura onde esses dados sejam processados ocorra de forma segura, utilizando algoritmos criptográficos para preservar o sigilo das informações;
6.4.22.5. Deverá ser feita a investigação e a classificação dos eventos monitorados, aplicando os principais frameworks de gestão de incidentes de segurança cibernética bem como boas práticas de mercado na detecção e triagem dos eventos de segurança, objetivando minimizar a presença de falsos positivos na abertura de incidentes de segurança;
6.4.22.6. O serviço de monitoramento deverá ser capaz de coletar e realizar a correlação de eventos dos sistemas e ativos monitorados, permitindo uma visão mais abrangente do alcance das ações maliciosas, bem como de possível movimentação lateral do atacante dentro da rede;
6.4.22.7. O monitoramento deverá ser capaz de identificar as principais ameaças, bem como táticas, técnicas e procedimentos de ataque descritos na base de conhecimento MITRE ATT&CK, sem prejuízo do uso de outras bases de conhecimento ou serviços de inteligência de ameaças, para complementação da capacidade de identificação de atividades maliciosas;
6.4.22.8. Deverá monitorar e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média e identificando comportamentos anômalos, visando antecipar a identificação de incidentes de segurança;
6.4.22.9. A solução deverá prover inteligência de proteção contra-ataques cibernéticos a nível global, sendo responsável por pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança monitorados;
6.4.22.10. O fabricante deverá utilizar solução para registro de incidente de segurança, acessível pela equipe técnica da Contratante, para indicar ações de contenção, comunicar à equipe da Contratante sobre o andamento do tratamento dos incidentes;

6.4.23. Compatibilidade:

6.4.23.1. É suportada por qualquer um dos seguintes navegadores:
6.4.23.1.1. Apple Safari versões mais recentes;
6.4.23.1.2. Google Chrome versões mais recentes;
6.4.23.1.3. Microsoft Edge;
6.4.23.1.4. Mozilla Firefox versões mais recentes;

6.4.24. Requisitos de rede:

6.4.24.1.1. Em condições médias de carga: um canal full-duplex com largura de banda de pelo menos 1,7 Kbps para cada ativo;
6.4.24.1.2. Em condições de carga máxima: um canal full-duplex com largura de banda de pelo menos 2,7 Kbps para cada ativo;

6.4.25. Compatibilidade de sensor de endpoint

6.4.25.1. O agente de endpoint deve ser compatível com os seguintes sistemas operacionais, para no mínimo a coleta e envio dos dados/telemetria ao SOC do fabricante:
6.4.25.1.1. Microsoft Windows 7 e superiores;
6.4.25.1.2. macOS 10.14-11;
6.4.25.1.3. CentOS 6.7 ou superior;
6.4.25.1.4. Debian GNU / Linux 9.4 ou superior;
6.4.25.1.5. Linux Mint 19 ou superior;
6.4.25.1.6. Oracle Linux 7.3 ou superior;
6.4.25.1.7. Red Hat Enterprise Linux 6.7 ou superior;
6.4.25.1.8. SUSE Linux Enterprise Server 12 SP5 ou superior;
6.4.25.1.9. Ubuntu 18.04 LTS ou superior.

6.4.26. Capacidades técnicas

6.4.26.1. Deve possuir console web própria do serviço, além de integração nativa com a console do “software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets”
6.4.26.2. A console deve possuir dashboards com as informações principais, apresentando no mínimo:
6.4.26.2.1. Número de incidentes e status
6.4.26.2.2. Quantidade de dispositivos monitorados
6.4.26.2.3. Deve possuir mecanismo de notificações, com no mínimo as seguintes opções:
6.4.26.2.4. E-mail
6.4.26.2.5. Telegram
6.4.26.3. Deve permitir o envio de relatórios;
6.4.26.4. O agente deve enviar a telemetria em tempo real para o SoC do fabricante;
6.4.26.5. O serviço deve compreender monitoramento dos dados enviados e alertas gerados em um regime 24x7x265;
6.4.26.6. O envio e armazenamento da telemetria, devem respeitar as principais legislações de proteção de dados, como GDPR e LGPD;
6.4.26.7. O SoC do fabricante deve possuir datacenters em pelo menos duas localidades em diferentes países;
6.4.26.8. O SoC do fabricante deve possuir equipes de analistas em pelo menos 3

regiões (países) incluindo Brasil;
6.4.26.9. Os dados coletados devem passar por no mínimo:
6.4.26.9.1. Modelos de Machine Learning/Inteligência Artificial;
6.4.26.9.2. Análise humana;
6.4.26.9.3. Correlação com IoA's (indicadores de ataque);
6.4.26.9.4. Emulação em sandbox (quando necessário);
6.4.26.10. Após análise, informações sobre atividades potencialmente maliciosas, devem ser apresentadas no portal como "Incidentes";
6.4.26.11. O Incidente deve possuir no mínimo as seguintes informações:
6.4.26.11.1. Resumo;
6.4.26.11.2. Prioridade (Baixa, Média e Alta);
6.4.26.11.3. Recomendação;
6.4.26.11.4. Data de criação e data de atualização;
6.4.26.11.5. Correlacionamento com táticas/técnicas do Framework MITRE ATT&CK;
6.4.26.11.6. Dispositivos afetados;
6.4.26.11.7. IOCs de host e de rede;
6.4.26.11.8. Descrição completa em linha do tempo;
6.4.26.12. O incidente pode receber ações de resposta recomendada disparadas pela equipe de SoC, compreendendo no mínimo as seguintes ações:
6.4.26.12.1. Transferir arquivo para o SoC;
6.4.26.12.2. Isolar um dispositivo;
6.4.26.12.3. Desabilitar isolamento de dispositivo;
6.4.26.12.4. Deletar chave de registro;
6.4.26.12.5. Dump de memória;
6.4.26.13. As ações devem ser aprovadas no portal por profissional da contratante, com a opção de habilitar aprovação automática.

6.4.27. Agente de endpoint

6.4.27.1. As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;
6.4.27.2. A solução deve oferecer módulo focado em capacidades de EDR "Endpoint Detection and Response", incluindo no mínimo as seguintes capacidades:
6.4.27.3. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;
6.4.27.4. Deve fornecer graficamente a visualização da cadeia do ataque;
6.4.27.5. Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).
6.4.27.6. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:
6.4.27.6.1. Isolar o host;
6.4.27.6.2. Iniciar uma varredura nas áreas críticas;
6.4.27.6.3. Quarentenar o objeto;
6.4.27.7. A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

6.4.27.7.1. Detecções provenientes da solução de endpoint;
6.4.27.7.2. Processos;
6.4.27.7.3. Alterações de registro;
6.4.27.7.4. Conexões remotas;
6.4.27.7.5. Criação de arquivos;
6.4.27.8. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.
6.4.27.9. Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução.
6.4.27.10. A solução deve oferecer no mínimo as seguintes opções de resposta:
6.4.27.10.1. Prevenir a execução de um arquivo;
6.4.27.10.2. Quarentenar um arquivo;
6.4.27.10.3. Iniciar uma varredura por IoC;
6.4.27.10.4. Parar um processo;
6.4.27.10.5. Executar um processo;
6.4.27.11. Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:
6.4.27.11.1. A opção de isolamento deve estar disponível junto a visualização do incidente;
6.4.27.11.2. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

ITEM 06 – SOFTWARE DE SEGURANÇA PARA STORAGE
6.4.28. Requerimentos Gerais

6.4.28.1. A solução deve possuir proteção AntiMalware em tempo real;
6.4.28.2. A solução deve ter a capacidade de proteger servidores de arquivos e servidores de armazenamentos conectados à rede (NAS);
6.4.28.3. Deve possuir gerenciamento, monitoramento e atualizações centralizados;
6.4.28.4. Deve ter a capacidade de conter padrões de ataques baseados em redes;
6.4.28.5. Deve nativamente possuir proteção contra criptografia de pastas e arquivos compartilhados;
6.4.28.6. Deve possuir suporte ao agente CAVA e aos protocolos RCP e ICAP;
6.4.28.7. Deve ser tolerante à falhas e ser escalável;
6.4.28.8. Deve suportar servidores em Cluster;
6.4.28.9. Deve possuir mecanismo de atualização do banco de dados de reputação de malwares, devendo ser do próprio fabricante da solução, com possibilidade de escolha da frequência.
6.4.28.10. Permitir a busca por vários métodos de atualização, incluindo canais de comunicação global e recursos compartilhados na rede local.
6.4.28.11. Permitir a verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
6.4.28.12. A console de gerenciamento do computador deve funcionar nas seguintes plataformas Windows
6.4.28.12.1. Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou superior (32 /64 bits);

6.4.28.12.2. Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou superior (32/64 bits);
6.4.28.12.3. Windows Server 2008 Standard / Enterprise / Datacenter SP2 ou superior (32 /64 bits);
6.4.28.12.4. Windows Server 2008 Core ou superior (64 bits);
6.4.28.12.5. Microsoft Small Business Server 2008 Standard / Premium SP2 ou superior (64 bits);
6.4.28.12.6. Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 ou superior (64 bits);
6.4.28.12.7. Windows Hyper-V Server 2008 R2 SP1 ou superior (64 bits);
6.4.28.12.8. Microsoft Small Business Server 2011 Essentials / Standard SP1 ou superior (64 bits);
6.4.28.12.9. Microsoft Windows MultiPoint Server 2011 Standard / Premium Microsoft Small Business Server 2008 Standard / Premium SP2 ou superior (64 bits);
6.4.28.12.10. Windows Server 2012 Foundation / Essentials / Standard / Datacenter (64 bits);
6.4.28.12.11. Microsoft Windows MultiPoint Server 2012 Standard / Premium (64 bits);
6.4.28.12.12. Windows Storage Server 2012 Foundation / Essentials / Standard / Datacenter (64bits);
6.4.28.12.13. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (64bits);
6.4.28.12.14. Windows Storage Server 2012 R2 (64bits);
6.4.28.12.15. Windows Hyper-V Server 2012, Windows Hyper-V Server 2012 R2 (64bits);
6.4.28.12.16. Windows Server 2016 Essentials / Standard / Datacenter (64bits);
6.4.28.12.17. Microsoft Windows MultiPoint Server 2016 (64bits);
6.4.28.12.18. Windows Storage Server 2016 Essentials / Standard / Datacenter (64bits);
6.4.28.12.19. Windows Server 2019 Essentials / Standard / Datacenter (64bits);
6.4.28.12.20. Windows Storage Server 2019 (64bits);
6.4.28.12.21. Microsoft Windows XP Professional SP2 ou superior (32/64 bits);
6.4.28.12.22. Microsoft Windows Vista (32/64 bits);
6.4.28.12.23. Microsoft Windows 7 (32/64 bits);
6.4.28.12.24. Microsoft Windows 8 ou superior (32/64 bits);
6.4.28.12.25. Microsoft Windows 10 (32/64 bits);
6.4.28.12.26. Windows 10 Redstone 1 à 6 (32/64 bits);

6.4.29. Características para Proteção de Servidores de Arquivos
6.4.29.1. Deve possuir Compatibilidade de instalação com os seguintes sistemas operacionais:
6.4.29.1.1. Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou superior (32 /64bits);
6.4.29.1.2. Windows Server 2003 R2 Foundation SP2 ou superior (32bits);
6.4.29.1.3. Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou superior (32/64 bits);
6.4.29.1.4. Windows Server 2008 Standard / Enterprise / Datacenter SP2 ou superior(32 /64bits);
6.4.29.1.5. Windows Server 2008 Core Standard / Enterprise / Datacenter SP2 ou superior

(32/64bits);
6.4.29.1.6. Microsoft Small Business Server 2008 Standard / Premium SP2 ou posterior (64 bits);
6.4.29.1.7. Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 ou posterior (64 bits);
6.4.29.1.8. Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 ou posterior (64 bits);
6.4.29.1.9. Windows Hyper-V Server 2008 R2 SP1 ou posterior (64 bits);
6.4.29.1.10. Microsoft Small Business Server 2011 Essentials / Standard SP1 ou posterior (64 bits);
6.4.29.1.11. Microsoft Windows MultiPoint Server 2011 Standard / Premium (64 bits);
6.4.29.1.12. Windows Server 2012 Foundation / Essentials / Standard / Datacenter (64 bits);
6.4.29.1.13. Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter (64 bits);
6.4.29.1.14. Microsoft Windows MultiPoint Server 2012 Standard / Premium (64 bits);
6.4.29.1.15. Windows Storage Server 2012 (64 bits);
6.4.29.1.16. Windows Hyper-V Server 2012 (64 bits);
6.4.29.1.17. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (64 bits);
6.4.29.1.18. Windows Server 2012 R2 Core / Foundation / Essentials / Standard / Datacenter (64 bits);
6.4.29.1.19. Windows Storage Server 2012 R2 (64 bits);
6.4.29.1.20. Windows Hyper-V Server 2012 R2 (64 bits);
6.4.29.1.21. Windows Server 2016 Essentials / Standard / Datacenter (64 bits);
6.4.29.1.22. Windows Server 2016 MultiPoint (64 bits);
6.4.29.1.23. Windows Server 2016 Core Standard / Datacenter (64 bits);
6.4.29.1.24. Microsoft Windows MultiPoint Server 2016 (64 bits);
6.4.29.1.25. Windows Storage Server 2016 (64 bits);
6.4.29.1.26. Windows Hyper-V Server 2016 (64 bits);
6.4.29.1.27. Windows Server 2019 Essentials / Standard / Datacenter (64 bits);
6.4.29.1.28. Windows Server 2019 Core (64 bits);
6.4.29.1.29. Windows Storage Server 2019 (64 bits);
6.4.29.1.30. Windows Hyper-V Server 2019 (64 bits);
6.4.29.1.31. Windows 10 Enterprise multi-session (64 bits);
6.4.29.2. A solução de segurança deve fornecer proteção aos servidores de arquivos usando os seguintes servidores de terminal:
6.4.29.2.1. Windows 2008 SP2 Server Microsoft Remote Desktop Services ou superior;
6.4.29.2.2. Windows 2008 R2 Server Microsoft Remote Desktop Services ou superior;
6.4.29.2.3. Windows 2012 Server Microsoft Remote Desktop Services ou superior;
6.4.29.2.4. Windows 2012 Server R2 Remote Desktop Services ou superior;
6.4.29.2.5. Windows 2016 Server Microsoft Remote Desktop Services ou superior;
6.4.29.2.6. Windows 2019 Server Microsoft Remote Desktop Services ou superior;
6.4.29.2.7. Citrix XenApp 6.0, 6.5, 7.0, 7.5 – 7.9, 7.15
6.4.29.2.8. Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15
6.4.29.3. Deve realizar a proteção contra malwares em tempo real e permitir a

configuração de verificação agendada;
6.4.29.4. Deve possuir proteção especial contra malware de criptografia de arquivos para recursos de rede compartilhados, fornecendo defesas confiáveis contra Ransomware;
6.4.29.5. Deve possibilitar a proteção baseada em nuvem contra novas ameaças, permitindo que o aplicativo entre em contato com os recursos especializados do fabricante para obter um veredicto de arquivo durante a verificação em tempo real ou programada;
6.4.29.6. Deve permitir a verificação manual ou sob demanda de servidores de arquivos selecionados;
6.4.29.7. Deve permitir o escaneamento de arquivos, pastas ou de todo o sistema selecionado;
6.4.29.8. Deve impedir o re-escanemento de arquivos;
6.4.29.9. Quando atuando no veredicto de um malware, deve no mínimo tomar as seguintes ações:
6.4.29.9.1. Bloquear;
6.4.29.9.2. Neutralização;
6.4.29.9.3. Remoção e,
6.4.29.9.4. Notificar os administradores.
6.4.29.10. Deve possuir uma console de gerenciamento única para todos os componentes de proteção;
6.4.29.11. Deve ter a capacidade de excluir arquivos, no mínimo, com as seguintes bases:
6.4.29.11.1. Um nome específico,
6.4.29.11.2. Arquivos localizados em um endereço específico e,
6.4.29.11.3. Arquivos com uma máscara específica.
6.4.29.12. Ter a capacidade importar ou exportar a lista de exclusões de verificação e proteção em tarefas de verificação e perfis de proteção;
6.4.29.13. Ter a capacidade de exportar e importar lista de exceções;
6.4.29.14. Ter a capacidade de criar lista de exceções frequentes compiladas de acordo com as recomendações da Microsoft;
6.4.29.15. Deve poder realizar o armazenamento de cópias de backup de arquivos excluídos;
6.4.29.16. Dar suporte para o esquema de licenciamento de acordo com a quantidade de servidores de segurança;
6.4.29.17. Ter suporte para ativação usando um código de ativação fornecido via assinatura;
6.4.29.18. Deve fornecer informações sobre o número de objetos escaneados;
6.4.29.19. Deve fornecer informações sobre detalhes do banco de dados de antivírus;

6.4.30. Características para Proteção de Servidores de Armazenamento conectados à rede (NAS)

6.4.30.1. A solução de suportar a integração com os seguintes servidores NAS:
6.4.30.1.1. NetApp® com um dos seguintes sistemas:
6.4.30.1.1.1. Data ONTAP 7.x and Data ONTAP 8.x 7-mode;
6.4.30.1.1.2. Data ONTAP 8.2.1 Cluster-mode;
6.4.30.1.1.3. Data ONTAP 9.0 – 9.7 Cluster-mode;
6.4.30.1.2. Dell EMC™ Celerra / VNX com os softwares a seguir:

6.4.30.1.2.1. EMC DART 6.0.36 ou mais recente;
6.4.30.1.2.2. Celerra Anti Virus Agent (CAVA) 4.5.2.3 ou mais recente;
6.4.30.1.3. Dell EMC Isilon with OneFS 7.0 ou mais recente;
6.4.30.1.4. Hitachi NAS (ICAP, RPC):
6.4.30.1.4.1. 12.0 ou mais recente para integração com ICAP;
6.4.30.1.4.2. 11.2 ou mais recente para integração com RPC;
6.4.30.1.5. IBM System Storage N series;
6.4.30.1.6. Oracle ZFS Storage Appliance;
6.4.30.1.7. Dell NAS na plataforma Dell Compellent™ FS8600:
6.4.30.1.7.1. FluidFS 6.x;
6.4.30.1.7.2. FluidFS 5.x;
6.4.30.1.8. HPE 3PAR com File Persona 3.3.1:
6.4.30.1.8.1. HPE 3PAR StoreServ File Controller;
6.4.30.1.8.2. HPE 3PAR StoreServ 7000c, 8000, 9000, 20000 Storage;
6.4.30.1.9. Nutanix File Storage:
6.4.30.1.9.1. Nutanix Files 3.8 ou posterior;
6.4.30.2. Deve realizar a proteção contra malwares em tempo real e permitir a configuração de verificação agendada;
6.4.30.3. Deve possibilitar a proteção baseada em nuvem contra novas ameaças, permitindo que o aplicativo entre em contato com os recursos especializados do fabricante para obter um veredicto de arquivo durante a verificação em tempo real ou programada;
6.4.30.4. Deve permitir a verificação manual ou sob demanda de servidores de arquivos selecionados;
6.4.30.5. Deve permitir o escaneamento de arquivos, pastas ou de todo o sistema selecionado;
6.4.30.6. Deve impedir o re-escanemento de arquivos;
6.4.30.7. Quando atuando no veredicto de um malware, deve no mínimo tomar as seguintes ações:
6.4.30.7.1. Bloquear;
6.4.30.7.2. Neutralização;
6.4.30.7.3. Remoção e,
6.4.30.7.4. Notificar os administradores.
6.4.30.8. Deve possuir uma console de gerenciamento única para todos os componentes de proteção;
6.4.30.9. Deve ter a capacidade de excluir arquivos, no mínimo, com as seguintes bases:
6.4.30.9.3. Arquivos com uma máscara específica.
6.4.30.10. Ter a capacidade importar ou exportar a lista de exclusões de verificação e proteção em tarefas de verificação e perfis de proteção;
6.4.30.11. Ter a capacidade de exportar e importar lista de exceções;
6.4.30.12. Ter a capacidade de criar lista de exceções frequentes compiladas de acordo com as recomendações da Microsoft;
6.4.30.13. Deve poder realizar o armazenamento de cópias de backup de arquivos excluídos;
6.4.30.14. Dar suporte para o esquema de licenciamento de acordo com a quantidade de

servidores de segurança;
6.4.30.15. Ter suporte para ativação usando um código de ativação fornecido via assinatura;
6.4.30.16. Deve fornecer informações sobre o número de objetos escaneados;
6.4.30.17. Deve fornecer informações sobre detalhes do banco de dados de antivírus;

ITEM 07 – SOFTWARE DE DETECÇÃO CONTRA-ATAQUES COMPLEXOS E DIRECIONADOS
6.4.31. Das capacidades da console de gerenciamento

6.4.31.1. A Console de gerenciamento deve apresentar uma dashboard customizável;
6.4.31.2. Deve apresentar a saúde do sistema, informando quais componentes estão atualizados ou não;
6.4.31.3. Deve mostrar em tempo real o tráfego sendo processado pelos sensores;
6.4.31.4. Deve apresentar em tempo real gráfico de pacotes descartados caso não suporte o tráfego gerado;
6.4.31.5. Deve permitir criar perfis de layout;
6.4.31.6. Deve permitir exportar para PDF o layout atual da solução;
6.4.31.7. Deve mostrar pelo menos as seguintes informações atualizadas sobre a ferramenta:
6.4.31.7.1. Saúde do sistema;
6.4.31.7.2. Tráfego em tempo real;
6.4.31.7.3. Top 10 domínios mais acessados;
6.4.31.7.4. Mostrar alertas por importância;
6.4.31.7.5. Top 10 Ips mais acessados;
6.4.31.7.6. Alertas por tecnologias de detecção;
6.4.31.7.7. Alertas por vetor de ataques;
6.4.31.8. Deve permitir criar novos usuários para acesso à console com pelo menos 3 níveis de acesso;
6.4.31.9. Deve permitir integração com a Console de gerenciamento da ferramenta de antivírus caso seja necessário a implementação de EDR;
6.4.31.10. Os alertas deverão ser exibidos permitindo visualizar quantos são novos, quantos estão em processo e quantos já foram processados;
6.4.31.11. Deve mostrar quantidades de eventos pela criticidade, alto, médio ou baixo;
6.4.31.12. Deve permitir exportar os alertas para o formato (.txt);
6.4.31.13. Possibilidade de assinalar um evento para determinado usuário para verificação;
6.4.31.14. Deve suportar arquivos no formato CEF para integração com SIEM;
6.4.31.15. O usuário com conta administrativa deve ter permissão para assinalar um incidente para usuários específicos;
6.4.31.16. Possibilidade de marcar evento como processado para informar que o incidente já foi analisado e resolvido;
6.4.31.17. Deve se possível gerenciar o status de cada evento;
6.4.31.18. As seguintes informações devem ser mostradas nos alertas de eventos:
6.4.31.18.1. Host onde ocorreu o incidente;

6.4.31.18.2. Origem do ataque;
6.4.31.18.3. Destino do ataque;
6.4.31.18.4. Dia e horário de quanto ocorreu o ataque;
6.4.31.18.5. Nome do objeto considerado malicioso;
6.4.31.18.6. Tamanho do objeto;
6.4.31.18.7. Hash do objeto em pelo menos MD5 e SHA256;
6.4.31.18.8. URL do ataque;
6.4.31.18.9. Nome da tecnologia responsável por identificar o ataque;
6.4.31.18.10. Informar se o ataque possui características baseado no YARA (Ferramenta open source);
6.4.31.18.11. A console de gerenciamento deverá permitir que o administrador procure por eventos similares na rede baseado no tipo de arquivo, no hash do arquivo, tipo de evento e nome do arquivo;
6.4.31.18.12. Deve permitir a instalação do sensor de endpoint de forma remota;
6.4.31.18.13. Possibilidade de mostrar a sequência de atividades executadas pelo malware quando executada no SandBox;
6.4.31.18.14. Deve permitir fazer uma busca no sistema por eventos baseados em regras;
6.4.31.18.15. Deve permitir fazer buscas de IoCs no banco de dados através de informações recebidas pelos agentes;
6.4.31.18.16. Deve permitir buscar no sistema eventos baseados nas seguintes categorias:
6.4.31.18.16.1. Texto completo;
6.4.31.18.16.2. Por host;
6.4.31.18.16.3. Por tipo de vento;
6.4.31.18.16.4. Por arquivos;
6.4.31.18.16.5. Pelo hash MD5 e SHA256;
6.4.31.18.16.6. Pela conexão de rede;
6.4.31.18.16.7. Chave de registro;
6.4.31.18.16.8. Eventos do Windows;
6.4.31.18.16.9. Alteração de nome do host;
6.4.31.18.17. Deve permitir importar IOCs (Índices de comprometimento) visando encontrar ataques de acordo com informações contidas no IoC;
6.4.31.18.18. Capacidade de executar as seguintes tarefas remotamente nos Endpoints que possuem o EDR (Endpoint Detection Response) instalado:
6.4.31.18.18.1. Finalizar processo;
6.4.31.18.18.2. Executar programa;
6.4.31.18.18.3. Coletar arquivo;
6.4.31.18.18.4. Deletar arquivo;
6.4.31.18.18.5. Quarentenar arquivo;
6.4.31.18.18.6. Restaurar arquivo da quarentena;
6.4.31.18.19. Deve permitir ao coletar um arquivo remotamente enviar automaticamente para o SANDBOX para análise;
6.4.31.18.20. Deve possuir funcionalidade que permita prevenir um arquivo de ser executado em qualquer host com o EDR instalado através do hash MD5/SHA256;
6.4.31.18.21. Deverá possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;

6.4.31.18.22. Deverá permitir o uso de base de conhecimento na Internet do próprio fabricante, com atualização automática de regras e assinaturas, para consultas automáticas em bases de reputação e correlacionamento de informações sobre ameaças conhecidas, identificando assim as respectivas recomendações de ações;
6.4.31.18.23. Deve possuir plataforma de inteligência de ameaças, informando se o ataque faz parte de uma campanha global, quais as regiões e plataformas afetadas pelo ataque, bem como disponibilizar links de referência sobre a ameaça;
6.4.31.18.24. Deve possuir plataforma do próprio fabricante com informações sobre as ameaças, informando título, data descoberta e descrição sobra a ameaça.
6.4.31.18.25. Deve possuir integração com portal de inteligência para avançar na pesquisa a partir dos eventos;
6.4.31.18.26. Deve ser possível realizar consultas de IP, HASH domínios no portal de inteligência do próprio fabricante;
6.4.31.18.27. Para cada malware, Exploits ou componente malicioso, a ferramenta deve possuir links para detalhar informações sobre estes;
6.4.31.18.28. Possibilidade de selecionar quais dispositivos serão afetados pela tarefa de prevenção de execução de arquivos;
6.4.31.18.29. Capacidade de baixar arquivos quarentenados diretamente pela console de administração do Anti-APT;
6.4.31.18.30. Capacidade de visualizar quantos Endpoints possuem o EDR instalado através de integração com a Console de gerenciamento do antivírus;
6.4.31.18.31. Deve mostrar quantos Endpoints estão sendo gerenciados informando também quantos não possuem EDR instalado;
6.4.31.18.32. Possuir relatórios customizáveis possibilitando adicionar ou remover colunas de identificação e status de ventos;
6.4.31.18.33. Deve permitir criar relatórios baseados na tecnologia de proteção utilizada;
6.4.31.18.34. Criar relatórios de eventos organizados pelas seguintes severidades: baixa, média e alta;
6.4.31.18.35. Deve permitir adicionar imagens ao relatório;
6.4.31.18.36. Permitir criar listas brancas baseadas nos seguintes filtros:
6.4.31.18.36.1. Por hash MD5;
6.4.31.18.36.2. Por formato;
6.4.31.18.36.3. Por URL;
6.4.31.18.36.4. Por e-mail;
6.4.31.18.36.5. Por Sub-rede;
6.4.31.18.37. Permitir criar regras de notificações para envio por e-mail quando novos eventos são identificados pela ferramenta;
6.4.31.18.38. Deve permitir configurar o status do endpoint de acordo com a quantidade de dias de inatividade;
6.4.31.18.39. Deve permitir integrar a solução com pelo menos as seguintes ferramentas de SIEM: ArchSight, Splunk e IBM Qradar;

6.4.32. Características para o SandBox

6.4.32.1. As Sandboxes deverão suportar os seguintes sistemas operacionais:
6.4.32.1.1. Windows XP x86 Sp3;
6.4.32.1.2. Windows 7 X64;

6.4.32.1.3. Windows 10 x64;
6.4.32.2. Suportar atualização da base de dados da Rede de Inteligência de forma automática e sem causar nenhum tipo de indisponibilidade da solução;
6.4.32.3. A análise inicial deve ser realizada de forma local no ambiente de detecção, o envio de artefatos para verificação na SandBox deve ocorrer de forma automática, ou seja, caso a inteligência do produto identifique a necessidade de encaminhar o objeto para análise na SandBox este processo deve ocorrer sem a intervenção de qualquer usuário;
6.4.32.4. A solução deve ser capaz de prover dados forense detalhados, via interface gráfica, relacionados à infecção, demonstrando o ciclo de vida completo do ataque. Estes dados forenses devem incluir a cronologia completa do ataque e não apenas uma porção do ataque, assim como:
6.4.32.4.1. URLs/sites web relacionados ao ataque;
6.4.32.4.2. hashes MD5/SHA256;
6.4.32.4.3. binários maliciosos anexados;
6.4.32.5. Detectar e inspecionar, no mínimo, os seguintes tipos de arquivo, considerando as diferentes versões de sistemas operacionais e aplicativos existentes:
6.4.32.5.1. Arquivos executáveis;
6.4.32.5.2. Scripts;
6.4.32.5.3. Arquivos;
6.4.32.5.4. Documentos do office;
6.4.32.5.5. Arquivos de mídia;
6.4.32.5.6. Arquivos de Android (APK)
6.4.32.6. A solução deverá prover um método de disponibilizar updates das Sandboxes sem requerer um completo update do sistema operacional ou upgrade da solução e sem indisponibilidade de sua detecção;
6.4.32.7. Toda análise básica de malwares, incluindo malwares desconhecidos, deve ser realizada de forma automatizada através da detecção do Exploits, sem a necessidade de criação de regras específicas ou interação de um operador;
6.4.32.8. Toda a análise do comportamento do malware deve ser registrada em tempo de execução;
6.4.32.9. A solução deve suportar importação de regras YARA personalizadas, para permitir flexibilidade na criação de regras para análise de ameaças;
6.4.32.10. Suportar mecanismo de whitelist pelos seguintes métodos:
6.4.32.10.1. Hash MD5 do arquivo;
6.4.32.10.2. Formato do arquivo;
6.4.32.10.3. E-mail;
6.4.32.10.4. Sub-rede.
6.4.32.11. Deve permitir o envio de alertas por e-mail;
6.4.32.12. A solução deverá suportar mais de um SandBox em cluster, permitindo o escalonamento baseado na necessidade do contratante;
6.4.32.13. Deverá possuir a capacidade de detectar ameaças direcionadas, realizando inspeção de tráfego até a camada 7 de forma a prevenir ataques do dia zero e executar análise profunda de documentos que contenham conteúdo malicioso ou redirecionamentos para outras URLs maliciosas;
6.4.32.14. O SandBox da solução deve possuir mecanismos para prevenção de evasão.

6.4.33. Sensores de detecção

6.4.33.1. A solução deverá permitir que o sensor monitore tráfego WEB, Mail e Rede;
6.4.33.2. Deverá permitir integração com solução de proxy utilizando o protocolo ICAP permitindo analisar protocolos seguros (exemplo: HTTPS);
6.4.33.3. Deverá verificar mensagens de e-mail através do protocolo POP3 e SMTP;
6.4.33.4. Deverá processar tráfego espelhado e extrair objetos e metadados do DNS
6.4.33.5. A solução deve suportar um throughput de análise de no máximo 4000 Mbps;
6.4.33.6. A solução deverá ser gerenciada por console Web suportando no mínimo os browsers Internet Explorer e Firefox;
6.4.33.7. Deve permitir configurar mais de um sensor de rede caso o ambiente corporativo tenha mais de um ponto para análise;
6.4.33.8. Deverá possuir a capacidade de atualizar as vacinas do sensor pela internet ou através da console de gerenciamento;
6.4.33.9. O Sensor de rede deverá suportar SPAN Port ou TAP para análise do tráfego;
6.4.33.10. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;
6.4.33.11. O sensor deverá encaminhar automaticamente para a SandBox um artefato potencialmente perigoso identificado no tráfego de rede;
6.4.33.12. O sensor deverá alertar qualquer artefato malicioso identificado já conhecido sem a necessidade de intervenção manual;
6.4.33.13. Deverá detectar incidentes de segurança motivados por conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos além da detecção de malwares conhecidos e desconhecidos, Ransomware, Exploits, Botnets, Cross Site Script, SQL Injection, comunicações p2p, Instant Messengers; streaming, tentativas de scan de rede, tentativas de brute-force, situações de evasão e roubo de informação etc.;
6.4.33.14. Deverá ter capacidade de verificar em tempo real a reputação de endereços web (URLs) e servidores de correio SMTP;
6.4.33.15. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística;
6.4.33.16. Deverá atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;
6.4.33.17. Deve permitir utilizar um sensor de rede como proxy, ou seja, deve permitir que o sensor receba informações do Endpoint para enviar à console de gerenciamento;
6.4.33.18. O Sensor deverá detectar sites maliciosos através de reputação;
6.4.33.19. O sensor deverá ter acesso a rede global de inteligência da fabricante;
6.4.33.20. Deverá integrar com a infraestrutura extraindo objetos do tráfego de rede e efetuando uma análise inicial;
6.4.33.21. Deverá receber objetos para serem verificados dos switches, servidores de proxy e servidores de e-mail;
6.4.33.22. Deverá atuar como IDS na rede detectando anomalias no tráfego de rede e alertando a console de gerenciamento sobre os eventuais incidentes;
6.4.33.23. Caso necessário, deve suportar uma arquitetura única atuando como sensor de rede e console de gerenciamento em uma mesma máquina virtual;
6.4.33.24. Através de consulta na base global da fabricante, deverá detectar os seguintes

itens:
6.4.33.24.1. Endereços envolvidos em campanhas de ataques persistentes;
6.4.33.24.2. Servidores de “Command & Control”;
6.4.33.24.3. Sites maliciosos;
6.4.33.24.4. Sites de phishing;
6.4.33.25. Deverá possuir tecnologia de cache para evitar envio de solicitações duplicadas;
6.4.33.26. Deve possuir capacidade de verificar links ativos em documentos do office;
6.4.33.27. O sensor de endpoint deve ser compatível com fabricantes terceiras, permitindo que colete e envie informações a console de gerenciamento sem causar conflito com a atual solução de antivírus.

ITEM 08 – SOFTWARE DE PREVENÇÃO CONTRA A PERDA DE DADOS
6.4.34. Gerenciamento da solução

6.4.34.1. A solução deve fornecer uma estrutura de política única em todos os canais de exfiltração de dados (por exemplo, e-mail, Web, aplicativos SaaS, Impressão, aplicações, Mídia Removível, Compartilhamento de Arquivos);
6.4.34.2. Todas as funções de gerenciamento, incluindo alterações de configuração e upgrades, devem ser conduzidas a partir de um console central;
6.4.34.3. O sistema deve apoiar o acesso baseado em funções e a administração delegada com funções pré-definidas e personalizáveis:
6.4.34.3.1. Auditor;
6.4.34.3.2. Gerente de Incidentes;
6.4.34.3.3. Gerente de Políticas;
6.4.34.3.4. Super Administrador;;
6.4.34.3.5. Administrador
6.4.34.4. A solução proposta deve oferecer suporte à integração com Active Directory ou File Directory (CSV);
6.4.34.5. A solução deve oferecer suporte à criação/exceção de política com base no diretório de usuário/grupo, máquina, rede, domínio;
6.4.34.6. A solução deve ter a capacidade de auditar alterações (por exemplo, logon/o, alterações de regras, logs do sistema, logs de tráfego);
6.4.34.7. Capacidade de o sistema notificar quando está tendo problemas de conexão;
6.4.34.8. Capacidade de integração (via syslog ou extração de banco de dados) com ferramentas de SIEM para fins de registro e alerta;
6.4.34.9. A solução deve fornecer escalabilidade futura para todos os componentes integrantes da arquitetura que compõe o sistema de DLP;
6.4.34.10. A solução deve oferecer suporte a ambientes de infraestrutura virtualizados, como Azure ou AWS para o portal de gerenciamento, banco de dados e outros componentes.
6.4.34.11. A solução deve ter integração nativa com Classificações de Dados (Boldon James, Microsoft AIP, Seclore, Titus).
6.4.34.12. A solução proposta deve ser capaz de implantar o agente usando métodos comuns de implantação de software, como GPO, SCCM, JAMF etc.
6.4.34.13. A solução deve fornecer a capacidade de verificar o status do agente e relatar

quaisquer agentes que não estejam funcionando corretamente;
6.4.34.14. As comunicações com os módulos da solução e sistemas integrados devem ser criptografadas, via https (entrada/saída);
6.4.34.15. A solução deve oferecer suporte ao Microsoft RMS;
6.4.34.16. A solução deve usar um banco de dados relacional corporativo, como SQL;
6.4.34.17. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, nos sistemas operacionais:
6.4.34.17.1. Windows Server 2008 R2 SP1;
6.4.34.17.2. Windows Server 2012;
6.4.34.17.3. Windows Server 2012 R2;
6.4.34.17.4. Windows Server 2016;
6.4.34.18. Liste os sistemas operacionais e o suporte de versão para Endpoints, VDI, Browsers etc.
6.4.34.19. A arquitetura da solução deve oferecer suporte a sites remotos e usuários de rede distribuídos em muitos locais diferentes.
6.4.34.20. A solução deve descrever em meios de implantação típicos e onde cada componente reside;
6.4.34.21. A solução deve oferecer suporte à autenticação de dois fatores para acesso do administrador ao console de gerenciamento;
6.4.34.22. A solução deve ter uma API RESTful disponível para incidentes de obtenção e atualização;
6.4.34.23. Solução deve ser capaz de ser implantada em Máquinas Virtuais AWS EC2 e Azure;
6.4.34.24. Configuração de políticas de segurança de dados e detecção de conteúdo confidencial;
6.4.34.24.1. A solução deve ter políticas específicas de conformidade "prontas para uso" com base na região e no tipo de setor;
6.4.34.24.2. A solução deve ter políticas pré-definidas (1500+) baseadas em RegEX, Dicionários ou Scripts e deve ser capaz de selecionar políticas com base na correlação do país
e das indústrias;
6.4.34.24.3. A solução deve fornecer políticas predefinidas para identificar possíveis expressões que sejam indicativas de cyberbullying, padrões autodestrutivos ou descontentamento dos funcionários;
6.4.34.24.4. A solução deve ter políticas de Indicadores de Risco de Roubo de Dados (por exemplo, e-mail para concorrentes, currículos etc.);
6.4.34.24.5. A solução deve ter a capacidade de usar uma única política para varrer os dados onde quer que sejam armazenados, transmitidos ou usados, tanto na rede quanto no terminal;
6.4.34.24.6. A solução deve permitir modificar os canais de destino podem para quaisquer políticas. (Exemplo: incluir em uma política utilizando o protocolo SMTP, poder incluir os protocolos HTTP e HTTPS;
6.4.34.24.7. Deve configurar exceções baseadas em regras de forma simples evitando geração de falsos positivos;
6.4.34.24.8. A solução deve permitir uma sintaxe exível para vincular dados a aplicativos

específicos, servidores de arquivos, compartilhamentos de rede, impressoras e padrões de conteúdo exclusivos;
6.4.34.24.9. A solução deve oferecer suporte a tipos de arquivo verdadeiros predefinidos;
6.4.34.24.10. A solução deve oferecer suporte a condições de políticas com base na lógica booleana (AND, OR, NOT);
6.4.34.24.11. A solução deve suportar dados confidenciais em diferentes idiomas, incluindo, mas não limitando o suporte para português do Brasil e Inglês;
6.4.34.24.12. A solução deve extrair e inspecionar o conteúdo baseado em texto de arquivos e anexos;
6.4.34.24.13. A solução deve analisar os metadados do arquivo;
6.4.34.24.14. A solução deve oferecer suporte a impressão digital de arquivo parcial e de hash completo para todos os canais de exfiltração de dados;
6.4.34.24.15. A solução deve distinguir entre diferentes tipos de PII ou PHI. Exemplo: Distinguir entre os nove dígitos sociais de um cliente (CPF) e número de segurança de um número de telefone de nove dígitos sem a presença de uma palavra-chave;
6.4.34.24.16. A solução deve suportar a inspeção de tipos de arquivos de arquivos (ZIP, TAR) para detectar o conteúdo com impressão digital;
6.4.34.24.17. A solução deve suportar a análise de arquivos e anexos grandes (20 MB e maiores) durante o processo de impressão digital do conteúdo;
6.4.34.24.18. A solução deve fornecer um método para dados de impressão digital, como registros de clientes (dados estruturados);
6.4.34.24.19. A solução deve proteger pelo menos 10 milhões de linhas de conteúdo específico de um banco de dados de informações confidenciais sem depender de palavraschave ou padrões;
6.4.34.24.20. A solução deve oferecer suporte a um método de detecção de aprendizado de máquina para códigos-fonte, formulários;
6.4.34.24.21. A solução deve suportar regras totalmente personalizáveis com expressões regulares, palavras-chave, frases-chave e dicionários;
6.4.34.24.22. A solução deve oferecer suporte ao conteúdo da lista de permissões para remover com segurança a detecção de conteúdo textual;
6.4.34.24.23. A solução deve oferecer suporte à detecção de várias palavras-chave com base em um peso especificado;
6.4.34.24.24. A solução deve suportar pelo menos 5.000 listas de palavras-chave exclusivas;
6.4.34.24.25. A solução deve suportar correspondência de padrões combinada com validação. Por exemplo, detectar padrões comuns de números de cartão de crédito como bem
como fazer a validação da soma de verificação para garantir um número de cartão de crédito válido;
6.4.34.24.26. A solução deve detectar formatos de arquivo criptografados conhecidos e desconhecidos;
6.4.34.24.27. A solução deve identificar tags de classificação de terceiros, Proteção de Informações do Azure ou outras soluções de classificação de dados;
6.4.34.25. Configuração de proteção para estações de trabalho:
6.4.34.25.1. O agente da solução deve ser compatível com MacOS e Windows OS;
6.4.34.25.2. O agente da solução deve ser compatível com Vmware Horizon e Citrix

XenApp;
6.4.34.25.3. O agente da solução deve fornecer proteção contínua de dados confidenciais, independentemente de o usuário estar dentro ou fora da rede. A última política aplicada deverá
ser sempre a política padrão;
6.4.34.25.4. A solução deve detectar tentativas do usuário de enviar dados confidenciais por e-mail e Web (HTTP/S);
6.4.34.25.5. A solução deve impedir que os usuários enviem dados confidenciais através de qualquer aplicativo no computador;
6.4.34.25.6. A solução deve impedir a exfiltração de dados por meio de mídia removível (por exemplo, unidades USB);
6.4.34.25.7. A solução deve ser capaz de aplicar políticas diferentes mesmo quando os usuários estão usando o mesmo endpoint;
6.4.34.25.8. As tarefas de descoberta de dados de endpoint devem ter uma opção de agendamento:
6.4.34.25.8.1. uma vez;
6.4.34.25.8.2. diariamente;
6.4.34.25.8.3. semanalmente;
6.4.34.25.8.4. continuamente
6.4.34.25.9. A tarefa de descoberta de dados de endpoint deve ter configurações exíveis para verificar apenas quando o computador estiver ocioso ou pausar a verificação enquanto o
computador estiver funcionando com baterias;
6.4.34.25.10. A tarefa de descoberta de dados deve oferecer suporte à inclusão e exclusão por tipo de arquivo, pastas, idade ou tamanho;
6.4.34.25.11. A tarefa de descoberta de dados deve oferecer suporte a opções de varredura completas e diferenciais;
6.4.34.25.12. A descoberta de dados deve ter uma opção para preservar o tempo de acesso original;
6.4.34.25.13. O agente da solução deve aproveitar as tags de rótulos de metadados MIP ou Boldon James para impor a classificação ou reclassificar quando um arquivo violar uma política
de dados em repouso
6.4.34.25.14. O agente precisa ser auto-regenerativo e resistente a adulterações;
6.4.34.25.15. Deve monitorar a área de transferência do sistema operacional e tomar medidas com base nos dados copiados e/ou protegidos;
6.4.34.25.16. A solução precisa oferecer suporte a opções de implantação de sistemas operacionais virtualizados;
6.4.34.25.17. O agente precisa oferecer uma mensagem pop-up que possa conter informações customizadas quando o usuário violar uma política;
6.4.34.25.18. A mensagem pop-up deve fornecer uma oportunidade para fornecer justificativa
comercial quando a política permitir esta ação;
6.4.34.25.19. A justificativa do usuário deve ser registrada/armazenada em um método que possa ser lido por outros sistemas";

6.4.34.25.20. Os arquivos copiados para dispositivos removíveis devem ser criptografados e o conteúdo deve ser legível apenas em ativos de propriedade da empresa;
6.4.34.25.21. O agente deve oferecer suporte à visibilidade de dados copiados para dispositivos de mídia removível específicos;
6.4.34.25.22. O agente da solução deve oferecer suporte à criptografia de nível de administrador e senha de auto criptografia para o usuário quando os arquivos são copiados para mídia removível;
6.4.34.25.23. O agente de endpoint precisa ter o mínimo ou nenhum impacto no desempenho
da máquina.
6.4.34.25.24. O agente da solução deve oferecer suporte a políticas hierárquicas de usuário /grupo com correção/resposta configuráveis;
6.4.34.25.25. O agente da solução deve ser compatível com os navegadores Edge Chromium, Firefox, Safari (Apple) e Chrome;
6.4.34.25.26. O agente da solução deve oferecer suporte ao monitoramento e bloqueio de dados confidenciais carregados para aplicativos em nuvem não autorizados e armazenamento
em nuvem;
6.4.34.25.27. O agente da solução deve oferecer suporte a um processo para desabilitar o agente do endpoint com autorização;
6.4.34.25.28. O agente da solução deve oferecer suporte à capacidade de confiar no aplicativo, configurando- o para não ser monitorado;
6.4.34.25.29. O agente da solução deve oferecer suporte às seguintes operações em dados confidenciais que podem ser executadas nas estações de trabalho:
6.4.34.25.29.1. Copiar e colar controles (ou seja, atividades da área de transferência);
6.4.34.25.29.2. Controle de impressão em impressoras locais ou de rede;
6.4.34.25.29.3. Salvar conteúdo em diferentes locais, incluindo salvar em:
6.4.34.25.29.4. Pastas locais;
6.4.34.25.29.5. Compartilhamentos de arquivos remotos;
6.4.34.25.29.6. Unidades removíveis conectadas a um sistema de endpoint, como unidades USB;
6.4.34.25.29.7. Salvar em locais de armazenamento em nuvem;
6.4.34.26. Configuração de proteção para Dados em Repouso:
6.4.34.26.1. A solução deve oferecer suporte à verificação de dados em repouso no endpoint;
6.4.34.26.2. A solução deve suportar SMB, NFS e CIFS para compartilhamentos de arquivos baseados em Windows e não Windows;
6.4.34.26.3. As tarefas de descoberta de dados devem ter uma opção de agendamento: uma vez, diariamente, semanalmente ou continuamente;
6.4.34.26.4. A tarefa de descoberta de dados deve oferecer suporte à inclusão e exclusão por tipo de arquivo, pastas, idade ou tamanho;
6.4.34.26.5. A tarefa de descoberta de dados deve oferecer suporte a opções de varredura diferencial e completa;
6.4.34.26.6. A descoberta de dados deve ter uma opção para preservar o tempo de acesso original;

6.4.34.26.7. A descoberta de dados deve oferecer suporte à alocação de largura de banda para verificação do processo de descoberta;
6.4.34.27. Gerenciamento de incidentes
6.4.34.27.1. A solução deve fornecer a capacidade de escalar incidentes críticos para gerentes ou proprietários de dados;
6.4.34.27.2. A solução deve fornecer controles de segurança e acesso em torno do caso /incidente (usuário e grupo);
6.4.34.27.3. A solução deve atribuir incidentes/casos a usuários de diferentes Unidades de Negócios;
6.4.34.27.4. A solução deve permitir a definição e o estabelecimento de uxos de trabalho específicos (ou seja, adicionar todos os três tipos de eventos aos casos), atribuir casos a usuários/proprietários individuais, permitir que os usuários adicionem notas etc;
6.4.34.27.5. A solução deve oferecer suporte ao monitoramento e gerenciamento de aspectos críticos e fases de cada incidente/caso e fases de cada incidente/caso até a resolução, envolvendo administradores autorizados especificados e usuários específicos da função, conforme necessário durante todo o processo;
6.4.34.27.6. A solução deve fornecer a capacidade de mostrar apenas determinados incidentes de um departamento específico ao ponto focal atribuído desse departamento;
6.4.34.27.7. A solução deve fornecer a capacidade de liberar automaticamente um e-mail em quarentena, postar a aprovação do gerente sem qualquer intervenção manual no console
DLP;
6.4.34.27.8. A solução deve oferecer suporte a scripts de correção para planos de ação de DLP (por exemplo, quando um arquivo viola as políticas de DLP, as soluções deixam um arquivo de exclusão com uma notificação);
6.4.34.27.9. A solução deve oferecer suporte ao Fluxo de Incidentes (Workow) via API para liberar e-mails de quarentena;

6.4.34.28. Relatórios

6.4.34.28.1. A solução deve permitir a investigação de incidentes envolvendo dados em repouso, dados em uso e dados em movimento a partir de um console de gerenciamento centralizado;
6.4.34.28.2. A solução deve fornecer resumo e agrupamento de relatórios personalizados em diferentes variáveis e atributos;
6.4.34.28.3. A solução deve suportar exportações de relatórios de incidentes via planilha, XML, PDF ou HTML;
6.4.34.28.4. A solução deve ter relatórios pré-definidos para auxiliar nas investigações;
6.4.34.28.5. A solução deve suportar a capacidade de salvar relatórios personalizados e filtros de incidentes;
6.4.34.28.6. A solução deve suportar a capacidade de definir permissões de relatórios por departamentos;
6.4.34.28.7. A solução deve usar análise de dados avançada para fornecer à sua equipe de operações de segurança um relatório de classificação de pilha sobre os principais riscos de segurança de dados em sua organização;
6.4.34.28.8. A solução deve ser capaz de gerar relatórios programados;

6.4.34.28.9. A solução deve fornecer relatórios exíveis de incidentes (diário, semanal, mensal, trimestral etc.);
6.4.34.28.10. A solução deve ser capaz de relatar o número de alertas gerados por destino;
6.4.34.28.11. A solução deve permitir que os usuários criem mensagens de alerta personalizáveis para administradores, usuários e gerentes de usuários;
6.4.34.28.12. A solução deve fornecer um catálogo de relatórios abrangente que forneça um "drill-down" para facilitar a investigação dos incidentes de maior risco;
6.4.34.28.13. A solução deve ser capaz de fornecer dados forenses dentro do mesmo registro de incidente.
6.4.34.28.14. A solução deve priorizar instantaneamente casos de níveis de risco alto a baixo com limites de pontuação de risco personalizáveis fornecidos em uma pilha de relatórios de classificação de risco de incidente;
6.4.34.28.15. A solução deve capturar dados de eventos com metadados apropriados (data /hora, usuário, protocolo);
6.4.34.28.16. A solução deve suportar um protocolo de cadeia de custódia;
6.4.34.28.17. A solução deve reter os logs por pelo menos um ano, se não for possível, a solução deve oferecer suporte ao arquivamento de incidentes;
6.4.34.28.18. A solução deve ter a capacidade de alterar a gravidade:
6.4.34.28.18.1. Alta;
6.4.34.28.18.2. Média;
6.4.34.28.18.3. Baixa
6.4.34.28.19. A solução deve ter a capacidade de alterar seu o status:
6.4.34.28.19.1. Novo;
6.4.34.28.19.2. Em Processo;
6.4.34.28.19.3. Fechado;
6.4.34.28.19.4. Falso Positivo;
6.4.34.28.19.5. Escalado.

ITEM 09 - CONTRATAÇÃO DE SOFTWARE DE MONITORAMENTO DE APLICAÇÕES E INFRAESTRUTURA DE REDES E SERVIDORES

6.4.35. Solução de monitoramento de aplicações e infraestrutura de redes e servidores, com tecnologia para mapear todos os dispositivos conectados à rede, criação de Mapas de Topologia, fornecendo uma visibilidade aprofundada tanto em ambientes locais quanto na nuvem.
6.4.36. Deverá fornecer insights detalhados de desempenho e integridade dos sistemas, identificação de gargalos e otimização de desempenho, gerenciamento de configurações, correlacionamento de dados usando técnicas de AIOps, emitir alertas quando ocorrem eventos importantes e criar relatórios personalizados para análise e tomada de decisões, contemplando:
6.4.37. Gerenciamento de redes que permite detectar, diagnosticar e resolver rapidamente problemas de desempenho e falhas de rede, simplificando a detecção, o diagnóstico e a resolução de problemas;
6.4.38. Informações sobre o tempo de resposta, disponibilidade e tempo de atividade de roteadores, switches e outros dispositivos habilitados SNMP;
6.4.39. Apresentação do desempenho em tempo real através de mapas de rede

navegáveis e dinâmicos por meio de estatísticas;
6.4.40. Deverá conter Painéis de controle, alertas, relatórios e orientações especializadas prontos para uso sobre os itens gerenciados;
6.4.41. Deverá realizar o descobrimento automático dos dispositivos de rede habilitados para SNMP/WMI;;
6.4.42. Implementação de Solução de caminho de rede (mapa de rede): Deverá executar uma análise e visibilidade profunda dos caminhos críticos de rede desde a origem até
o destino mostrando visualmente o tráfego de cada nó (passo a passo);
6.4.43. Apresentação da pilha de desempenho com objetivo de correlacionar os dados e acelerar a identificação da causa raiz, de forma intuitiva através das métricas de desempenho diretamente em um cronograma para correlação visual imediata entre todos os
dados;
6.4.44. Captura dos dados de fluxos contínuos de tráfego de rede e apresentar em gráficos de fácil interpretação e tabelas que quantificam exatamente como a rede corporativa
está sendo usada e com que finalidade;
6.4.45. Oferecer uma visão ampla e personalizável do seu tráfego de rede em uma só console/página;
6.4.46. Analisar dados do NetFlow, J-Flow, sFlow, IPFIX e Huawei NetStream™ nos principais dispositivos de mercado como: Cisco Systems®, Extreme Networks®, HP®, Juniper®, Nortel Networks® e outros grandes fornecedores;
6.4.47. Informações sobre quais aplicativos estão consumindo mais da largura de banda da rede;
6.4.48. Oferecer notificações de alertas instantâneos, seus principais comunicadores, quando uma interface excede seu limite de utilização de largura de banda;
6.4.49. Capacidade de rastrear, gerenciar e planejar o uso de endereços IP e outros recursos relacionados em um ambiente de rede;
6.4.50. Permitir que os administradores executem a administração de serviços de DNS (Sistema de Nomes de Domínio) e Protocolo de Configuração Dinâmica de Host (DHCP), que atribuem e resolvem endereços IP para máquinas;
6.4.51. Fornecimento de funções para agilizar o processo de gerenciamento de endereços IP, com a capacidade de controlar as reservas de endereços IP em DHCP, agregação de dados e relatórios;
6.4.52. Rastreamento e monitoramento dos dados, desde endereços IP atualmente em uso até os dispositivos e usuários associados a esses endereços.
6.4.53. Centralizar o monitoramento de dados em uma única console, o software de gerenciamento de IP deverá fornecer insights críticos sobre elementos de gerenciamento de rede para acelerar a solução de problemas, planejamento de endereços IP e relatórios;
6.4.54. Gerenciamento dos riscos e requisitos de acesso à rede associados ao aumento dos dispositivos IP, oferecendo rastreamento automatizado de usuários e dispositivos,
juntamente com recursos avançados de gerenciamento de portas de switch, para controlar, usuários e dispositivos que estão conectados na rede;

6.4.55. A solução deverá ter aos gerenciamentos mínimas listadas abaixo:

6.4.55.1. Gerenciamento de LOGs:
6.4.55.1.1. Deve ser capaz de aceitar Syslog, traps SNMP e eventos do Windows de servidores e dispositivos de rede;
6.4.55.1.2. Deve fornecer console interativo para visualizar dados de eventos;
6.4.55.1.3. Deve fornecer console interativo para exibir eventos em tempo real;
6.4.55.1.4. Deve fornecer recurso de pesquisa rápida em eventos;
6.4.55.1.5. Deve permitir a personalização de filtros para restringir os resultados da pesquisa;
6.4.55.1.6. Deve permitir a marcação de eventos com tags codificadas por cores;
6.4.55.1.7. Deve oferecer suporte a regras personalizadas para descartar mensagens indesejadas;
6.4.55.1.8. Deve oferecer suporte a condições de alerta personalizadas com escopo de fonte de alerta personalizável;
6.4.55.1.9. Deve apoiar a execução de programa externo como ações de alerta;
6.4.55.1.10. Deve ter regras internas para uso imediato e para personalização;
6.4.55.1.11. Deve suportar o encaminhamento de alerta para a solução de monitoramento NOC ou outros sistemas;
6.4.55.1.12. Deve ter integração do Microsoft Active Directory para contas de usuário;
6.4.55.1.13. Deve fornecer um painel dinâmico que permita visibilidade detalhada e correlacione o syslog com pontos de dados históricos diferentes em diferentes partes da infraestrutura. O resultado deve ser exportável com um formato tabular;
6.4.55.1.14. A solução de gerenciamento de logs proposta deve se integrar diretamente às soluções de monitoramento e exibir dados de log junto com o desempenho da rede e dos sistemas no mesmo painel;
6.4.55.1.15. A solução de monitorização proposta deve proporcionar a capacidade de armazenamento a longo prazo e de recuperação das mensagens de registo originais;
6.4.55.2. Gerenciamento de Configuração do Servidor:
6.4.55.2.1. A solução de gerenciamento proposta deve ser capaz de fazer backup automático da configuração baseada em texto em sistemas baseados no Windows;
6.4.55.2.2. Deve detectar e exibir alterações para os seguintes itens:
6.4.55.2.2.1. Arquivo de configuração do aplicativo;
6.4.55.2.2.2. Inventário de hardware;
6.4.55.2.2.3. Inventário de software;
6.4.55.2.2.4. Registro do Windows;
6.4.55.2.2.5. Arquivo baseado em texto;
6.4.55.2.2.6. Arquivo binário;
6.4.55.2.3. Deve disparar alerta quando a alteração de configuração acontecer, com a comparação de quais linhas de configuração foram adicionadas, excluídas e modificadas;
6.4.55.2.4. Deve permitir que a configuração da linha de base seja usada como ponto de referência para comparação de alterações de configuração;
6.4.55.2.5. Deve permitir a comparação da configuração atual com a do passado para entender as mudanças ocorridas ao longo do tempo;

6.4.55.2.6. Deve detectar e exibir alterações no inventário de hardware, incluindo, mas não limitado a:
6.4.55.2.6.1. Processadores;
6.4.55.2.6.2. Módulos de memória;
6.4.55.2.6.3. Discos rígidos;
6.4.55.2.6.4. Controladores de armazenamento;
6.4.55.2.6.5. Placa de vídeo;
6.4.55.2.6.6. Interfaces de rede;
6.4.55.2.6.7. Mídia removível;
6.4.55.2.7. Deve detectar e exibir alterações no inventário de software, incluindo, mas não limitado a:
6.4.55.2.7.1. Software instalado;
6.4.55.2.7.2. Atualizações do sistema operacional;
6.4.55.2.7.3. Firmware;
6.4.55.2.7.4. Drivers;
6.4.55.2.8. A solução de gerenciamento proposta deve ser capaz de descobrir servidores na rede na entrada de:
6.4.55.2.8.1. Intervalos de endereços IP;
6.4.55.2.8.2. Sub-redes;
6.4.55.2.8.3. Endereços IP individuais;
6.4.55.2.9. Deve ter opção para ativar/desativar a adição automática de nós descobertos;
6.4.55.2.10. Deve fornecer informações de fim de vida/fim de suporte (EoL/EoS) para ajudar a manter os dispositivos atualizados em relação à contratação e manutenção da implantação;
6.4.55.2.11. Deve fornecer um painel dinâmico que permita visibilidade aprofundada e correlatos de pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável com um formato tabular;
6.4.55.2.12. Deve permitir o acesso remoto a recursos e funções relacionados ao trabalho e permitir o acesso remoto para editar e atualizar as configurações do dispositivo;
6.4.55.2.13. Deve permitir que vários usuários façam login ao mesmo tempo;
6.4.55.2.14. Deve fornecer seções separadas para tarefas de gerenciamento de configuração, inventário e relatórios sobre violações de políticas;
6.4.55.2.15. Deve destacar rapidamente dispositivos que não foram copiados para configuração, aqueles com conflitos na configuração etc.;
6.4.55.2.16. Deve se integrar ao Active Directory® para fins de login do usuário;
6.4.55.2.17. A solução de gestão proposta deve fornecer relatórios prontos para uso para várias estatísticas monitoradas;
6.4.55.2.18. Deve permitir a personalização de relatórios adicionando/removendo colunas, definindo filtros, especificando prazos, agrupando colunas etc.;
6.4.55.2.19. Deve permitir que os relatórios sejam enviados dentro do cronograma como relatórios diários, semanais e mensais;
6.4.55.2.20. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;
6.4.55.2.21. Deve ser capaz de fazer backup da configuração, executar script de configuração e mostrar as últimas alterações de configuração como ações de alerta;

6.4.55.2.22. Deve ter várias ações disponíveis, incluindo, mas não limitado a envio de emails, encaminhamento de traps SNMP, execução de executáveis, envio de alertas de texto SMS, reprodução de som, envio de e-mail para uma página da Web, etc.
6.4.55.2.23. A solução de gerenciamento proposta deve permitir o agrupamento de dispositivos por várias propriedades:
6.4.55.2.23.1. por fornecedor;
6.4.55.2.23.2. tipo de máquina; versão do sistema operacional;
6.4.55.2.23.3. outras propriedades personalizadas;
6.4.55.2.24. Deve ser capaz de integrar com módulos que servem outros fins de monitoramento e fornecer uma visão de painel único
6.4.55.2.25. Deve oferecer suporte a várias opções de implantação:
6.4.55.2.25.1. Implantação centralizada;
6.4.55.2.25.2. Implantação distribuída;
6.4.55.2.25.3. Implantação híbrida;
6.4.55.2.26. Com uma exibição centralizada do console de operações, confirmação de alertas e interface de relatórios;
6.4.55.3. Monitoramento de desempenho:
6.4.55.3.1. A solução de monitoramento proposta deve ser capaz de monitorar:
6.4.55.3.1.1. Roteadores;
6.4.55.3.1.2. Switches;
6.4.55.3.1.3. Firewalls;
6.4.55.3.1.4. Dispositivos sem fio;
6.4.55.3.1.5. Servidores;
6.4.55.3.1.6. Outros dispositivos habilitados para SNMP;
6.4.55.3.2. Deve fornecer automaticamente estatísticas de desempenho de rede aprofundadas e em tempo real após a descoberta/configuração de dispositivos, incluindo, entre
outros:
6.4.55.3.2.1. Carga de CPU;
6.4.55.3.2.2. Utilização de memória;
6.4.55.3.2.3. Utilização da interface;
6.4.55.3.2.4. Perda de pacotes
6.4.55.3.3. Deve mostrar estatísticas como largura de banda da interface, tráfego atual em bps, total de bytes recebidos/transmitidos etc.;
6.4.55.3.4. Deve ser capaz de descobrir e solucionar problemas de caminhos de rede com detalhes, tanto para ambientes locais quanto na nuvem, de conexões TCP específicas;
6.4.55.3.5. Deve exibir informações que incluem emissão de alertas dos principais protocolos de roteamento (BGP, OSPF, RIP, EIGRP) com opções para exibir e pesquisar tabelas de roteamento, incluindo VRFs, mudanças em rotas padrão e rotas oscilantes, topologia de roteadores e status de vizinhos;
6.4.55.3.6. Deve ajudar com o monitoramento de informações de tráfego multicast e emissão de alertas que incluem informações de topologia, informações multicast, informações
de rotas, erros de multicast etc;
6.4.55.3.7. Deve exibir o status de dispositivos e da interface usando cores diferentes para

representar status de aviso e críticos;
6.4.55.3.8. Deve monitorar a integridade do hardware de fornecedores populares como Cisco, DELL, F5, Juniper, HP etc. e deve permitir emissão de alertas e relatórios sobre o monitoramento da integridade do hardware;
6.4.55.3.9. Deve mostrar detalhes, tanto em tempo real quanto históricos, na forma de gráficos e com a opção de escolha de períodos de tempo;
6.4.55.3.10. Deve ser capaz de descobrir e monitorar tanto dispositivos IPv4 quanto IPv6;
6.4.55.3.11. Deve ter opções de sondagem usando SNMP v1, v2c e v3 e WMI;
6.4.55.3.12. Deve ter opções para configurar os intervalos de sondagem, conforme necessário;
6.4.55.3.13. Deve ter opções para especificar períodos de retenção de dados;
6.4.55.3.14. Deve ter a opção para determinar a disponibilidade dos dispositivos usando somente SNMP;
6.4.55.3.15. A solução de monitoramento proposta deve ser capaz de descobrir dispositivos na rede automaticamente com recursos SNMP e ICMP, mediante o fornecimento de:
6.4.55.3.15.1. intervalos de endereços IP;
6.4.55.3.15.2. sub-redes;
6.4.55.3.15.3. endereços IP individuais;
6.4.55.3.15.4. Active Directory;
6.4.55.3.16. A solução não deve adicionar dispositivos com vários endereços IP como nós duplicados, mas relacionar todos os endereços IP conhecidos do nó;
6.4.55.3.17. Deve permitir a filtragem da interface quanto aos resultados da descoberta para excluir interfaces e portas de acesso virtuais e selecionar interfaces com base na correspondência de padrões;
6.4.55.3.18. Deve ter a opção de automatizar e agendar o processo de descoberta;
6.4.55.3.19. Deve ser capaz de importar automaticamente dispositivos descobertos;
6.4.55.3.20. Deve sinalizar na console a descoberta de novos dispositivos na rede;
6.4.55.3.21. Deve usar informações descobertas para criar mapas de topologia;
6.4.55.3.22. A solução de gerenciamento proposta deve fornecer uma interface gráfica de usuário de alta qualidade com atualização assíncrona da exibição;
6.4.55.3.23. Deve fornecer uma visão unificada de alertas, interceptações, eventos, mensagens Syslog em uma única página;
6.4.55.3.24. Deve oferecer uma única visão unificada de informações de multicast, informações de rotas e informações de dispositivo de um dispositivo;
6.4.55.3.25. Deve realçar rapidamente dispositivos com problemas, com base em diferentes propriedades, como tempo de resposta, carga da CPU, uso de memória, alto uso da
interface etc.;
6.4.55.3.26. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em dispositivos ou interfaces (ou seja, seu acesso deve ser baseado em funções);
6.4.55.3.27. Deve registrar no console Web, para fins de auditoria, ações de usuários e eventos, que devem ficar disponíveis para emissão de alertas e relatórios;
6.4.55.3.28. Deve permitir a elaboração interativa de gráficos de nó, interface, volume etc.;
6.4.55.3.29. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e

correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável em um formato tabular;
6.4.55.3.30. Deve integrar-se ao Active Directory para fins de login de usuários;
6.4.55.3.31. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;
6.4.55.3.32. Deve ser capaz de gerar/criar o relatório via console Web;
6.4.55.3.33. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;
6.4.55.3.34. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definição de filtros, especificação de períodos de tempo, agrupamento de colunas etc;
6.4.55.3.35. Deve permitir a personalização avançada pelo fornecimento de opções para inserir consultas personalizadas diretas ao banco de dados;
6.4.55.3.36. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá-los no console Web;
6.4.55.3.37. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;
6.4.55.3.38. Deve permitir o envio por e-mail de painéis criados no console Web;
6.4.55.3.39. Deve ser capaz de configurar tanto gráficos quanto tabelas em um único relatório;
6.4.55.3.40. Deve ter opções para importar/exportar relatórios criados por outros usuários;
6.4.55.3.41. A solução de monitoramento proposta deve ser capaz de gerenciar e exibir eventos/alertas no console Web;
6.4.55.3.42. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;
6.4.55.3.43. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;
6.4.55.3.44. Deve permitir a inserção de consultas personalizadas para criar regras a serem aplicadas ao banco de dados;
6.4.55.3.45. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;
6.4.55.3.46. Deve permitir a criação de alertas com base em estados sustentados;
6.4.55.3.47. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e-mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da
Web por e-mail etc.;
6.4.55.3.48. Deve ter a capacidade de estabelecer dinamicamente a linha de base de estatísticas e definir automaticamente o limite de alertas críticos e de aviso;
6.4.55.3.49. Deve permitir a supressão de alertas durante a manutenção programada;
6.4.55.3.50. A solução de monitoramento proposta deve permitir o agrupamento de dispositivos segundo diversas propriedades:
6.4.55.3.50.1. por departamento;
6.4.55.3.50.2. por local;
6.4.55.3.50.3. por nome;
6.4.55.3.50.4. por outras propriedades coletadas;

6.4.55.3.51. Deve ser capaz de definir dependências e relacionamentos entre dispositivos conectados e interfaces para evitar alertas de falso positivo por e-mail em caso de interrupção;
6.4.55.3.52. A solução de monitoramento proposta deve ser capaz de representar a rede pictoricamente e exibir detalhes de desempenho de dispositivos em tempo real;
6.4.55.3.53. Deve permitir a personalização de planos de fundo, ícones etc. e deve permitir que vários mapas de rede sejam aninhados com recurso de busca detalhada;
6.4.55.3.54. Deve ser capaz de exibir não apenas o status do dispositivo no mapa, mas também o status de qualquer outro detalhe obtido por meio da sondagem MIB personalizada;
6.4.55.3.55. Deve ter a capacidade de exibir o status de nós ou de um grupo agregado de nós por meio de dados dinamicamente atualizados;
6.4.55.3.56. Deve ser capaz de conectar dispositivos automaticamente por meio de informações de topologia reunidas durante a descoberta, como Cisco Discovery Protocol ou Link Layer Discovery Protocol;
6.4.55.3.57. Deve ser capaz de exibir a topologia multicast usando informações das listas de dispositivos upstream e downstream;
6.4.55.3.58. Deve ser capaz de exibir a localização geográfica de dispositivos;
6.4.55.3.59. Os dispositivos descobertos devem ser detectados como sendo de um fornecedor específico e categorizados automaticamente;
6.4.55.3.60. A solução de monitoramento proposta deve permitir a reunião de propriedades personalizadas de dispositivos habilitados para SNMP ao especificar o OID das propriedades;
6.4.55.3.61. Deve ser capaz de obter propriedades de dispositivos sem a necessidade de importar MIBs de dispositivos para o banco de dados MIB;
6.4.55.3.62. Deve ser capaz de obter, em tempo real, valores, gráficos e alertas dessas propriedades personalizadas;
6.4.55.3.63. Deve ter APIs disponíveis para importar/exportar nós programaticamente e executar funcionalidades semelhantes;
6.4.55.3.64. Deve ser capaz de fornecer o Tempo de resposta da rede (NRT) e o Tempo de resposta do aplicativo (ART) de aplicativos críticos;
6.4.55.3.65. Deve contar com identificação e classificação pronta para uso de ~1.200 aplicativos;
6.4.55.3.66. Deve ter a capacidade de exibir métricas de volumes agregados por aplicativo /nó;
6.4.55.3.67. Deve ser capaz de fornecer contextualmente dados QoE de nós na sub exibição Detalhes do nó;
6.4.55.3.68. Deve ter utilitários para exibir o banco de dados e para interromper e iniciar serviços de aplicativos;
6.4.55.3.69. Deve ter opções para receber, exibir e gerar alertas de interceptações e mensagens Syslog de dispositivos;
6.4.55.3.70. Deve ter a opção de criação de relatórios sem fio para exibir pontos de acesso sem fio finos e autônomos e seus clientes associados;
6.4.55.3.71. Deve ter exibições móveis personalizadas do console para visualização imediata por administradores;
6.4.55.3.72. Deve ser capaz de monitorar switches, pilha de energia e anéis de pilha de

dados de membros individuais nas pilhas de switches da Cisco;
6.4.55.3.73. Deve ser capaz de criar relatórios sobre tecnologias como Cisco UCS, recurso Energywise;
6.4.55.3.74. Deve ser capaz de criar relatórios sobre switches Cisco Nexus 1000V virtualizados, VSAN, switches Fibre Channel, como dispositivos Cisco MDS, Brocade, McData;
6.4.55.3.75. Deve ser capaz de monitorar toda a infraestrutura virtual VMware e Hyper-V, incluindo centrais virtuais, datacenters e clusters ESX, bem como rastrear automaticamente o
desempenho das VMs;
6.4.55.3.76. Deve ser capaz de monitorar componentes individuais no ambiente de balanceamento de carga F5 BIG-IP;
6.4.55.3.77. Deve ser capaz de monitorar componentes individuais no firewall Cisco ASA, incluindo, entre outros, contagem de conexões, túneis VPN entre sites e por acesso remoto, identidade e utilização de interfaces, status de alta disponibilidade e status de sincronização de
configuração.;
6.4.55.3.78. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;
6.4.55.3.79. Deve permitir a integração com aplicativos de terceiros na camada de interface do usuário, por meio de troca de mensagens e também de APIs;
6.4.55.3.80. A solução de monitoramento proposta deve ser capaz de acomodar o crescimento da rede pela adição de aplicativos de balanceamento de carga;
6.4.55.3.81. Deve permitir que informações de várias instâncias do aplicativo sejam consolidadas em uma única exibição;
6.4.55.4. Monitoramento de largura de banda:
6.4.55.4.1. A solução de monitoramento proposta deve ser capaz de monitorar o tráfego de rede pela captura de dados de fluxo de dispositivos de rede, incluindo Cisco NetFlow v5 ou
v9, Juniper J-Flow, IPFIX, sFlow, dados de NetStream, amostras de dados de NetFlow e Cisco ASA NetFlow;
6.4.55.4.2. Deve identificar quais usuários, aplicativos e protocolos estão consumindo mais largura de banda;
6.4.55.4.3. Deve realçar os endereços IP dos principais consumidores de largura de banda na rede e descobrir o uso indesejado de largura de banda;
6.4.55.4.4. Deve ser capaz de associar o tráfego vindo de diferentes fontes a nomes de aplicativos;
6.4.55.4.5. Deve ser capaz de receber fluxos de dispositivos que não estejam habilitados para SNMP, como VMware vSwitch;
6.4.55.4.6. Deve monitorar a qualidade de serviço baseada em classe (CBQoS) para descobrir se as políticas de priorização de tráfego são eficazes e se os aplicativos críticos para o negócio têm prioridade no tráfego da rede;
6.4.55.4.7. Também deve dar suporte às políticas de CBQoS aninhado;
6.4.55.4.8. Deve monitorar Tipo de serviço (ToS), Ponto de código diferenciado de serviços (DSCP) e Comportamento por salto (PHB);
6.4.55.4.9. Deve monitorar informações de BGP;

6.4.55.4.10. Deve mostrar detalhes tanto recentes quanto históricos na forma de gráficos com a opção de escolha de períodos de tempo;
6.4.55.4.11. Deve ter opções para especificar períodos de retenção de dados para evitar tensão no banco de dados e nos recursos de servidor;
6.4.55.4.12. Deve fornecer análise de fluxo com granularidade de um minuto e dar suporte a um fluxo sustentado de 60k por segundo;
6.4.55.4.13. A solução de monitoramento proposta deve ser capaz de adicionar automaticamente fontes de fluxo cujo desempenho já esteja sendo monitorado;
6.4.55.4.14. Deve notificar os fluxos que chegam de dispositivos e/ou interfaces não gerenciados e permitir sua adição para monitoramento com mínimo esforço;
6.4.55.4.15. A solução de gerenciamento proposta deve fornecer uma interface gráfica de usuário de alta qualidade;
6.4.55.4.16. Deve fornecer diversas exibições, categorizadas por usuário, aplicativo, departamento, conversa, interface, protocolo, tipo de serviço, Redes de sistemas autônomos;

6.4.55.4.17. Deve permitir a criação de exibições personalizadas do tráfego de rede, fornecendo uma lista de parâmetros para seleção na definição de filtros;
6.4.55.4.18. Deve ter a capacidade de salvar exibições filtradas personalizadas como novos links na página da Web para facilitar o acesso posteriormente, com opções para pesquisar intervalos IP/CIDR etc.;
6.4.55.4.19. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável em um formato tabular;
6.4.55.4.20. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em dispositivos ou interfaces (ou seja, seu acesso deve ser baseado em funções);
6.4.55.4.21. Deve integrar-se ao Active Directory para fins de login de usuários;
6.4.55.4.22. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;
6.4.55.4.23. Relatórios de qualidade de serviço baseada em classe devem fornecer detalhes sobre Pré-política, Pós-política e Abandonos;
6.4.55.4.24. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;
6.4.55.4.25. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definição de filtros, especificação de períodos de tempo, agrupamento de colunas etc;
6.4.55.4.26. Deve permitir a personalização avançada pelo fornecimento de opções para inserir consultas SQL diretas ao banco de dados;
6.4.55.4.27. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá-los no console Web;
6.4.55.4.28. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;
6.4.55.4.29. Deve permitir o envio por e-mail de painéis criados no console Web;
6.4.55.4.30. A solução de monitoramento proposta deve ser capaz de exibir eventos e alertas no console Web;

6.4.55.4.31. Alertas de qualidade de serviço baseada em classe (CBQoS) devem ser acionados quando o tráfego processado exceder os limites definidos para Pré-política, Póspolítica e Abandonos.;
6.4.55.4.32. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;
6.4.55.4.33. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;
6.4.55.4.34. Deve permitir a inserção de consultas SQL para criar regras a serem aplicadas ao banco de dados;
6.4.55.4.35. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;
6.4.55.4.36. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e-mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da
Web por e-mail etc.;
6.4.55.4.37. A solução de monitoramento proposta deve permitir a criação de grupos de endereços IP personalizados para categorizar fluxos por região, departamento, tipo de dispositivo etc.;
6.4.55.4.38. Deve ser capaz de usar esses grupos ao criar exibições personalizadas do tráfego de rede;
6.4.55.4.39. Deve ser capaz de fornecer uma visão resumida unificada levando em conta todos os dispositivos monitorados de diferentes fornecedores;
6.4.55.4.40. A solução de monitoramento proposta deve permitir a reunião de informações de fluxo de dispositivos que não sejam capacitados para fluxo quando usados com exportadores de fluxo de terceiros;
6.4.55.4.41. Deve ajudar na localização e no isolamento de computadores infectados em caso de ataque por vírus;
6.4.55.4.42. Deve dar importância às conversas com uso intensivo de banda larga para melhorar o desempenho do banco de dados, reduzir os tempos de carregamento de páginas e
aumentar a velocidade de criação de relatórios;
6.4.55.4.43. Deve permitir a resolução de DNS e NetBIOS de nomes de domínio de pontos de extremidade;
6.4.55.4.44. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;
6.4.55.4.45. Deve permitir a integração com aplicativos de terceiros na camada de interface do usuário, por meio de troca de mensagens e também de APIs;
6.4.55.4.46. A solução de monitoramento proposta deve ser capaz de monitorar até 3 milhões de fluxos por segundo, devendo empregar métodos avançados de otimização;
6.4.55.4.47. Deve ser capaz de acomodar o crescimento da rede pela adição de aplicativos de balanceamento de carga;
6.4.55.4.48. Deve permitir que informações de várias instâncias do aplicativo sejam consolidadas em uma única exibição;
6.4.55.5. Gerenciamento de configurações:

6.4.55.5.1. A solução de gerenciamento proposta deve ser capaz de fazer automaticamente o backup da configuração (tanto de arquivos de configuração baseados em
texto quanto binários) em roteadores, switches, firewalls, pontos de acesso e outros dispositivos de rede;
6.4.55.5.2. Deve ser capaz de fazer alterações em massa a configurações. Por exemplo, alterar cadeias de caracteres comunitárias, atualizar ACLs etc. em vários dispositivos;

6.4.55.5.3. Deve enviar alertas em tempo real quando acontecerem alterações à configuração da rede, com a comparação de quais linhas de configuração foram adicionadas, excluídas ou modificadas;
6.4.55.5.4. Deve permitir a comparação de arquivos de configuração de inicialização e execução para solucionar problemas de configuração de dispositivos;
6.4.55.5.5. Deve permitir a comparação da configuração atual com a do passado para permitir o entendimento das alterações que aconteceram ao longo do tempo;
6.4.55.5.6. Deve ajudar a automatizar tarefas repetidas pela definição de séries de comandos como modelos e sua execução com ou sem parâmetros;
6.4.55.5.7. Deve detectar violações da política de configuração para garantir a conformidade com regulamentações federais e padrões corporativos;
6.4.55.5.8. Deve automatizar o processo de aprovação de alterações permitindo ao administrador avaliar as alterações enviadas por carregadores antes de serem executadas nos
dispositivos;
6.4.55.5.9. Deve fornecer um inventário do hardware de dispositivos de rede e contar com relatórios prontos para uso de ativos e números de série;
6.4.55.5.10. Deve manter os dispositivos atualizados como parte da contratação e manutenção com rastreamento de suporte e fim da vida útil;
6.4.55.5.11. Deve ser compatível com vários protocolos, incluindo SNMP v1/v2c/v3, Telnet, SSH v1/v2 e TFTP;
6.4.55.5.12. Deve permitir a especificação de informações de login, protocolos de transferência e portas de transferência nos níveis global e de dispositivo;
6.4.55.5.13. A solução de gerenciamento proposta deve ser capaz de descobrir dispositivos na rede, mediante o fornecimento de:
6.4.55.5.13.1. intervalos de endereços IP;
6.4.55.5.13.2. sub-redes;
6.4.55.5.13.3. endereços IP individuais
6.4.55.5.14. Deve ter a opção de habilitar/desabilitar a adição automática dos nós descobertos;
6.4.55.5.15. Deve fornecer informações de Fim da vida útil/Fim do suporte (EoL/EoS) para ajudar a manter os dispositivos atualizados com relação à contratação e manutenção da implantação;
6.4.55.5.16. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável em um formato tabular;
6.4.55.5.17. Deve permitir o acesso remoto a recursos e funções relacionados a trabalhos,

devendo também permitir o acesso remoto para atualizar configurações de dispositivos;
6.4.55.5.18. Deve fornecer seções separadas para tarefas de gerenciamento de configuração, inventário e relatórios sobre violações das políticas;
6.4.55.5.19. Deve realçar rapidamente dispositivos com violações da políticas, dispositivos cujo backup da configuração não tenha sido feito, dispositivos com conflitos na configuração etc;
6.4.55.5.20. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em dispositivos ou interfaces (ou seja, seu acesso deve ser baseado em funções);
6.4.55.5.21. Deve integrar-se ao Active Directory para fins de login de usuários;
6.4.55.5.22. A solução de gerenciamento proposta deve fornecer relatórios prontos para uso de diversas estatísticas monitoradas;
6.4.55.5.23. Deve ter relatórios de políticas criados para regulamentações especificadas em HIPAA, SOX, CISCP, Cisco Security Audit etc.
6.4.55.5.24. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definição de filtros, especificação de períodos de tempo, agrupamento de colunas etc;
6.4.55.5.25. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;
6.4.55.5.26. Deve permitir o envio por e-mail de painéis criados no console Web;
6.4.55.5.27. A solução de gerenciamento proposta deve ser capaz de exibir eventos e alertas no console Web;
6.4.55.5.28. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;
6.4.55.5.29. Deve ser capaz de fazer backup da configuração, executar o script de configuração, mostrar alterações à última configuração como ações de alertas;
6.4.55.5.30. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e-mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da
Web por e-mail etc.;
6.4.55.5.31. A solução de gerenciamento proposta deve permitir o agrupamento de dispositivos segundo diversas propriedades:
6.4.55.5.31.1. por fornecedor;
6.4.55.5.31.2. tipo de máquina;
6.4.55.5.31.3. imagem de sistema operacional;
6.4.55.5.31.4. versão do sistema operacional;
6.4.55.5.31.5. resultado do último login;
6.4.55.5.31.6. outras propriedades personalizadas;
6.4.55.5.32. Os dispositivos descobertos devem ser detectados como sendo de um fornecedor específico e categorizados automaticamente;
6.4.55.5.33. A solução de gerenciamento proposta deve permitir a criação ou modificação de modelos de comandos para dispositivos que não contem com suporte pronto para uso;
6.4.55.5.34. Deve permitir a criação de modelos de dispositivos personalizados para automatizar tarefas de configuração repetidas;
6.4.55.5.35. Deve ser capaz de criar relatórios de políticas personalizados especificando o

conteúdo que deve ou não estar presente na configuração. O conteúdo pode ser especificado
como uma sequência de caracteres ou uma expressão regular;
6.4.55.5.36. Deve ter opções para receber, exibir e gerar alertas de interceptações e mensagens Syslog de dispositivos;
6.4.55.5.37. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;
6.4.55.5.38. A solução de gerenciamento proposta deve ser capaz de gerenciar até 10.000 dispositivos e acomodar o crescimento da rede pela adição de aplicativos de balanceamento de carga;
6.4.55.6. Monitoramento de WAN e VOIP:
6.4.55.6.1. A solução de monitoramento proposta deve ser capaz de identificar problemas de desempenho de rede específicos a sites ou relacionados à WAN usando a tecnologia Cisco IP SLA, além de monitorar caminhos de chamada VoIP para garantir a qualidade do serviço do
tráfego de voz;
6.4.55.6.2. Deve fornecer automaticamente estatísticas aprofundadas de desempenho de VoIP em tempo real, incluindo MOS, tremulação, latência de rede e perda de pacotes;
6.4.55.6.3. Deve ajudar a determinar o impacto do desempenho da WAN nos principais aplicativos;
6.4.55.6.4. Deve exibir o status de operações IP SLA usando cores diferentes para representar status de aviso e críticos;
6.4.55.6.5. Deve monitorar dados CDR/CMR para monitoramento de qualidade de chamada em tempo real e coleta de dados granulares, além de usar esses dados em alertas e
relatórios;
6.4.55.6.6. Deve ajudar a pesquisar chamadas VoIP e exibir detalhes de chamadas VoIP, chamadas com falha, chamadas da região, detalhes da região, causas de desconexão, chamadas por região, detalhes de telefone VoIP, detalhes do caminho, detalhes de gateway /ponto de extremidade VoIP etc.;
6.4.55.6.7. Deve ter opções para pesquisar registros de chamadas VoIP para localizar e solucionar problemas de chamadas problemáticas;
6.4.55.6.8. Deve fazer o monitoramento em tempo real da utilização de troncos PRI VoIP em gateways PRI da Cisco, fornecendo interface do usuário de distribuição de dados, gráficos de utilização de troncos e estatísticas históricas de utilização de VoIP e dados de gateways;
6.4.55.6.9. Deve mostrar detalhes, tanto em tempo real quanto históricos, na forma de gráficos e com a opção de escolha de períodos de tempo;
6.4.55.6.10. Deve ter opções para configurar os intervalos de sondagem, conforme necessário;
6.4.55.6.11. Deve ter opções para especificar períodos de retenção de dados;
6.4.55.6.12. A solução de monitoramento proposta deve ser capaz de descobrir dispositivos capacitados para IP SLA e fornecer a opção de adicioná-los diretamente ao monitoramento;
6.4.55.6.13. Esse console Web deve mostrar detalhes de gateways, como principais problemas de qualidade de chamadas de cada gateway, lista de todas as chamadas com falhas relacionadas a um gateway e utilização percentual atual de cada tronco;

6.4.55.6.14. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável em um formato tabular;
6.4.55.6.15. Deve permitir a personalização por contar com opções para adicionar/remover seções em página da Web, conforme necessário;
6.4.55.6.16. Deve realçar rapidamente operações com problemas, com base em diferentes propriedades, como latência, tremulação, MOS etc.;
6.4.55.6.17. Deve integrar-se ao Active Directory para fins de login de usuários
6.4.55.6.18. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;
6.4.55.6.19. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;
6.4.55.6.20. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definição de filtros, especificação de períodos de tempo, agrupamento de colunas etc.;
6.4.55.6.21. Deve permitir a personalização avançada pelo fornecimento de opções para inserir consultas SQL diretas ao banco de dados;
6.4.55.6.22. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá-los no console Web;
6.4.55.6.23. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;
6.4.55.6.24. Deve permitir o envio por e-mail de painéis criados no console Web;
6.4.55.6.25. A solução de monitoramento proposta deve ser capaz de exibir eventos e alertas no console Web;
6.4.55.6.26. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;
6.4.55.6.27. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;
6.4.55.6.28. Deve permitir a inserção de consultas SQL para criar regras a serem aplicadas ao banco de dados;
6.4.55.6.29. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;
6.4.55.6.30. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e-mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da
Web por e-mail etc.;
6.4.55.6.31. A solução de monitoramento proposta deve permitir o agrupamento de dispositivos segundo diversas propriedades – por local, por departamento, por nome e por outras propriedades coletadas;
6.4.55.6.32. A solução de monitoramento proposta deve ser capaz de representar a rede pictoricamente e exibir detalhes de dispositivos e operações em tempo real;
6.4.55.6.33. Deve permitir a personalização de planos de fundo, ícones etc. e deve permitir que vários mapas de rede sejam aninhados com recurso de busca detalhada;
6.4.55.6.34. A solução de monitoramento proposta deve dar suporte a operações IP SLA populares, incluindo: HTTP, FTP, DNS, DHCP, Conexão TCP, Tremulação UDP, Tremulação

VoIP UDP, Eco ICMP, Eco UDP, Eco de caminho ICMP, Tremulação de caminho ICMP;
6.4.55.6.35. Deve ter utilitários para exibir o banco de dados e para interromper e iniciar serviços de aplicativos;
6.4.55.6.36. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;
6.4.55.6.37. A solução de monitoramento proposta deve ser capaz de acomodar novos locais pela adição de aplicativos de balanceamento de carga;
6.4.55.7. Gerenciamento de endereços IP, DNS, DHCP:
6.4.55.7.1. A solução de monitoramento proposta deve ser capaz de gerenciar tarefas e conflitos de espaços de endereços IP usando uma interface do usuário centralizada baseada na Web;
6.4.55.7.2. Deve emitir um alerta antes do preenchimento de uma sub-rede ou escopo de DHCP;
6.4.55.7.3. Deve verificar endereços IP automaticamente e atualizar seu status;
6.4.55.7.4. Deve mostrar quais sub-redes estão próximas à capacidade total e como estão alocadas;
6.4.55.7.5. Deve permitir a definição de grupos e de segmentações para verificação;
6.4.55.7.6. Deve alocar automaticamente sub-redes corretamente dimensionadas especificando os tamanhos de super-redes e sub-redes;
6.4.55.7.7. Deve ter detecção ativa de conflitos de endereços IP, tanto em ambientes estáticos quanto DHCP;

6.4.55.7.8. Deve rastrear endereços IP historicamente e mostrar a alteração das propriedades ao longo do tempo;
6.4.55.7.9. Deve rastrear endereços IPv4 e IPv6 pela execução de uma pesquisa global;
6.4.55.7.10. Deve dar suporte ao gerenciamento e monitoramento de BIND DNS, permitindo a criação, modificação e exclusão de zonas DNS e registros DNS do BIND DNS v8. x, v9.x e v9.11+;
6.4.55.7.11. Deve monitorar o status do serviço BIND DNS e o status das zonas;
6.4.55.7.12. Deve ajudar no planejamento da migração para IPv6;
6.4.55.7.13. Deve permitir servidores DHCP de vários fornecedores – Windows, Cisco IOS e ISC;
6.4.55.7.14. A solução de monitoramento proposta deve permitir a importação de endereços IP a partir de planilhas;
6.4.55.7.15. Deve permitir a adição em massa de sub-redes, adicionando servidores DHCP e servidores DNS;
6.4.55.7.16. Deve usar o Microsoft Active Directory para fazer login no console Web;
6.4.55.7.17. Deve permitir a personalização por contar com opções para adicionar/remover seções em página da Web, conforme necessário;
6.4.55.7.18. Deve realçar rapidamente dispositivos com problemas, como os que apresentam uma alta porcentagem de portas utilizadas;
6.4.55.7.19. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em dispositivos ou interfaces (ou seja, seu acesso deve ser baseado em funções);
6.4.55.7.20. A solução de monitoramento proposta deve fornecer relatórios atuais e

históricos prontos para uso de diversas estatísticas monitoradas;
6.4.55.7.21. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;
6.4.55.7.22. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definição de filtros, especificação de períodos de tempo, agrupamento de colunas etc.;
6.4.55.7.23. Deve permitir a personalização avançada pelo fornecimento de opções para inserir consultas SQL diretas ao banco de dados;
6.4.55.7.24. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá-los no console Web;
6.4.55.7.25. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;
6.4.55.7.26. Deve permitir o envio por e-mail de painéis criados no console Web;
6.4.55.7.27. A solução de monitoramento proposta deve ser capaz de exibir eventos e alertas no console Web;

6.4.55.7.28. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;
6.4.55.7.29. Deve alertar quando houver um conflito de endereços IP com base no endereço MAC, quando os escopos DHCP se sobrepuserem a um endereço IP existente, quando houver uma alta utilização de sub-redes etc.;
6.4.55.7.30. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;
6.4.55.7.31. Deve permitir a inserção de consultas SQL para criar regras a serem aplicadas ao banco de dados;
6.4.55.7.32. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;
6.4.55.7.33. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e-mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da
Web por e-mail etc.;
6.4.55.7.34. A solução de monitoramento proposta deve permitir o agrupamento de dispositivos segundo diversas propriedades:
6.4.55.7.34.1. por departamento;
6.4.55.7.34.2. por local;
6.4.55.7.34.3. por nome;
6.4.55.7.34.4. e por outras propriedades coletadas;
6.4.55.7.35. Deve permitir a adição dinâmica de membros a grupos pela especificação de uma propriedade capaz de alterar valores dinamicamente, como volumes que estejam ficando
com pouco espaço livre;
6.4.55.7.36. Deve ser capaz de definir relacionamentos entre dispositivos conectados e interfaces para evitar alertas de falso positivo por e-mail em caso de interrupção;
6.4.55.7.37. A solução de monitoramento proposta não deve ser específica a um fornecedor;

6.4.55.7.38. A solução de monitoramento proposta deve ser capaz de localizar todos os pontos de extremidade em uma sub-rede;
6.4.55.7.39. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;
6.4.55.7.40. Deve integrar-se ao software de monitoramento de portas para mostrar informações de portas e usuários juntamente com o histórico de hosts de endereços IP ou de
atribuição de DNS;
6.4.55.7.41. Deve permitir o desligamento remoto de portas em caso de conflitos de endereços IP devido à integração;
6.4.55.7.42. Deve fornecer um pacote VMO para integrar-se ao VMware vRealize Orchestrator para proporcionar automação do fluxo de trabalho:
6.4.55.7.42.1. Simplificar o gerenciamento de endereços IP nas VMs;
6.4.55.7.42.2. Automatizar o provisionamento de endereços IP às VMs;
6.4.55.7.42.3. Automatizar o monitoramento de registros DNS das VMs;
6.4.55.7.43. Deve fornecer APIs para integração com produtos de terceiros;
6.4.55.7.44. A solução de monitoramento proposta deve ser capaz de acomodar o crescimento da rede pela adição de aplicativos de balanceamento de carga;
6.4.55.8. Monitoramento de portas de Switch:
6.4.55.8.1. A solução de monitoramento proposta deve ser capaz de rastrear a localização atual de um dispositivo ao obter seu endereço IP, nome de host ou endereço MAC;
6.4.55.8.2. Deve ajudar a localizar dispositivos invasores de maneira fácil e rápida;
6.4.55.8.3. Deve localizar portas de rede disponíveis;
6.4.55.8.4. Deve alertar quando um dispositivo específico se conecta, observando seu endereço MAC ou nome de host;
6.4.55.8.5. Deve mostrar as últimas localizações conhecidas (switch e porta) de um dispositivo desconectado;
6.4.55.8.6. Deve descobrir switches que estejam funcionando próximo da capacidade máxima para justificar a compra de novos equipamentos;
6.4.55.8.7. Deve mostrar cada porta de um switch para recuperar portas que não estejam em uso;
6.4.55.8.8. Deve monitorar os controladores quanto a pontos de acesso sem fio e pontos de acesso dinâmicos conectados a tais controladores;
6.4.55.8.9. Deve ter a opção de configurar uma lista branca de dispositivos com base em endereço MAC, endereço IP ou nome de host;
6.4.55.8.10. Deve sondar dispositivos quanto a dados de VRF;
6.4.55.8.11. Deve ter a opção de desligar portas remotamente;
6.4.55.8.12. Deve permitir a adição de um controlador de domínio do Active Directory para rastrear a atividade de logon na rede de usuários associados ao Active Directory;
6.4.55.8.13. Deve facilitar a coleta de informações de login de usuário configurando o nível de registro em log apropriado nos servidores Windows;
6.4.55.8.14. Deve ser capaz de rastrear clientes VPN conectados ao Cisco ASA;
6.4.55.8.15. A solução de monitoramento proposta deve ser capaz de descobrir dispositivos, bem como de descobrir portas nesses dispositivos;
6.4.55.8.16. Deve ter opções de filtragem avançadas durante a descoberta de portas (como

filtragem baseada em status, tronco, intervalo de portas, VLAN etc.) para reduzir o número de
portas que precisam ser ativamente monitoradas;
6.4.55.8.17. A solução de gerenciamento proposta deve fornecer uma interface gráfica de usuário de alta qualidade;
6.4.55.8.18. Deve permitir a personalização por contar com opções para adicionar/remover seções em página da Web, conforme necessário;
6.4.55.8.19. Deve realçar rapidamente dispositivos com problemas, como os que apresentam uma alta porcentagem de portas utilizadas;
6.4.55.8.20. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em dispositivos ou interfaces (ou seja, seu acesso deve ser baseado em funções);
6.4.55.8.21. Deve integrar-se ao Active Directory para fins de login de usuários;
6.4.55.8.22. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;
6.4.55.8.23. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;
6.4.55.8.24. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definição de filtros, especificação de períodos de tempo, agrupamento de colunas etc.;
6.4.55.8.25. Deve permitir a personalização avançada pelo fornecimento de opções para inserir consultas SQL diretas ao banco de dados;
6.4.55.8.26. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá-los no console Web;
6.4.55.8.27. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;
6.4.55.8.28. Deve permitir o envio por e-mail de painéis criados no console Web;
6.4.55.8.29. A solução de monitoramento proposta deve ser capaz de exibir eventos e alertas no console Web;
6.4.55.8.30. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;
6.4.55.8.31. Deve alertar quando um novo endereço MAC aparece na rede, quando aparece um nome de host na rede que não consta da lista branca e quando um item que está
sendo observado fica ativo;
6.4.55.8.32. Deve alertar quando um ponto de extremidade é alterado;
6.4.55.8.33. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;
6.4.55.8.34. Deve permitir a inserção de consultas SQL para criar regras a serem aplicadas ao banco de dados;
6.4.55.8.35. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;
6.4.55.8.36. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e-mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da

Web por e-mail etc.;
6.4.55.8.37. A solução de monitoramento proposta deve permitir o agrupamento de dispositivos segundo diversas propriedades:
6.4.55.8.37.1. por departamento;
6.4.55.8.37.2. por local;
6.4.55.8.37.3. por nome;
6.4.55.8.37.4. e por outras propriedades coletadas;
6.4.55.8.38. Deve permitir a adição dinâmica de membros a grupos pela especificação de uma propriedade capaz de alterar valores dinamicamente, como volumes que estejam ficando
com pouco espaço livre;
6.4.55.8.39. Deve ser capaz de definir relacionamentos entre dispositivos conectados e interfaces para evitar alertas de falso positivo por e-mail em caso de interrupção;
6.4.55.8.40. A solução de monitoramento proposta não deve ser específica a um fornecedor;
6.4.55.8.41. Os dispositivos descobertos devem ser detectados como sendo de um fornecedor específico e categorizados automaticamente;
6.4.55.8.42. A solução de monitoramento proposta deve ser capaz de localizar todos os pontos de extremidade em uma sub-rede;
6.4.55.8.43. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;
6.4.55.8.44. A solução de monitoramento proposta deve ser capaz de acomodar o crescimento da rede pela adição de aplicativos de balanceamento de carga;
6.4.55.9. Monitoramento de aplicativos:
6.4.55.9.1. A solução de monitoramento proposta deve ser capaz de monitorar:
6.4.55.9.1.1. Status de aplicativos;
6.4.55.9.1.2. Estatísticas de desempenho de aplicativos;
6.4.55.9.1.3. Serviços e processos;
6.4.55.9.1.4. Desempenho do sistema operacional;
6.4.55.9.1.5. Hardware;
6.4.55.9.2. Deve fornecer automaticamente uma visão em tempo real dos processos em execução nos sistemas e estatísticas aprofundadas do desempenho de aplicativos após sua descoberta/configuração;
6.4.55.9.3. Deve ser capaz de gerenciar processos, serviços em execução nos sistemas e estatísticas aprofundadas do desempenho de aplicativos após sua descoberta/configuração;
6.4.55.9.4. Deve fornecer automaticamente uma visão em tempo real de logs de eventos do Windows, incluindo o nível dos logs de eventos, a identificação do evento e sua fonte;
6.4.55.9.5. Deve ter métodos de monitoramento especializados que indicam o status e o desempenho dos principais parâmetros dos aplicativos (como serviços, comprimento da fila no
caso do Exchange, consultas SQL no caso de bancos de dados etc.) com base em práticas recomendadas;
6.4.55.9.6. Deve ser capaz de reunir importantes parâmetros de um aplicativo em um único modelo de monitoramento que possa ser uniformemente aplicado a aplicativos em diferentes servidores;

6.4.55.9.7. Uma personalização feita no modelo de monitoramento de um aplicativo deve ser propagada imediatamente para todos os outros servidores que tenham o aplicativo;
6.4.55.9.8. Deve permitir o uso de scripts personalizados com diversas opções de mecanismo de script, como VBscript, Perl, Powershell etc.;
6.4.55.9.9. Deve ter opções de monitoramento da experiência do usuário com diversos aplicativos e serviços, como HTTP, FTP, DHCP, DNS, SQL Server, Oracle, JSON, etc. para descobrir problemas, antes mesmo que os usuários se deem conta deles;
6.4.55.9.10. Deve ser capaz de criar relatórios com detalhes de hardware (como CPU, memória, estado de ventiladores, alimentação etc.) de servidores de fornecedores populares,
como IBM, HP, DELL, bem como hosts VMware;
6.4.55.9.11. Deve ter opções de sondagem usando SNMP, WMI e outros métodos;
6.4.55.9.12. Deve exibir o status de aplicativos e de serviços importantes usando cores diferentes para representar status de aviso e críticos;
6.4.55.9.13. Deve mostrar detalhes, tanto em tempo real quanto históricos, na forma de gráficos e com a opção de escolha de períodos de tempo;
6.4.55.9.14. Deve ter opções para configurar os intervalos de sondagem, conforme necessário;
6.4.55.9.15. Deve ser capaz de obter métricas de desempenho de E/S de disco de processos e serviços monitorados via WMI;
6.4.55.9.16. Deve ter opções para especificar períodos de retenção de dados;
6.4.55.9.17. Deve ser capaz de fornecer Registro em logs de eventos de auditoria de usuário, incluindo:
6.4.55.9.17.1. Processos encerrados;
6.4.55.9.17.2. Serviços parados / iniciados / reiniciados / Nós reinicializados;
6.4.55.9.17.3. Credenciais e gabaritos de aplicativos recém-criados / editados / excluídos;
6.4.55.9.17.4. Aplicativos atribuídos, removidos, gerenciados e não gerenciados;
6.4.55.9.18. Deverá possuir recurso de monitoramento de nuvem para:
6.4.55.9.18.1. Descobrir e monitorar instâncias EC2 na nuvem via API;
6.4.55.9.18.2. Descobrir e monitorar volumes EBS via API;
6.4.55.9.18.3. Descobrir e monitorar o serviço de nuvem via API;
6.4.55.9.18.4. Descobrir e monitorar novas instâncias automaticamente;
6.4.55.9.18.5. Consolidar a exibição de sistemas em nuvem, híbridos e locais;
6.4.55.9.18.6. Monitorar o desempenho de aplicativos e métricas de sistema operacional em instâncias na nuvem;
6.4.55.9.19. A solução de monitoramento proposta deve ser capaz de descobrir aplicativos nos servidores escolhidos, aplicar o monitoramento a eles e dar início a estatísticas para relatório em alguns minutos;
6.4.55.9.20. Deve ter uma opção para localizar processos por WMI ou SNMP, Monitores de contador de desempenho, Monitores WMI, Monitores de contador de desempenho do VMware
etc.;
6.4.55.9.21. Deve ter uma opção para localizar monitores JMX para monitoramento de aplicativos baseados em Java, como JBoss, Tomcat, WebLogic etc.;
6.4.55.9.22. Deve ser capaz de descobrir servidores de e-mail e diretório, bancos de dados,

serviços de rede, sistemas operacionais, servidores VMware ESX etc. automaticamente por meio de modelos de monitoramento incorporados;
6.4.55.9.23. Deve ser capaz de criar e definir o cálculo automático de limites críticos e de aviso a partir de dados de linha de base;
6.4.55.9.24. Deve fornecer monitoramento aprofundado (AppInsight) e pronto para uso do Microsoft SQL com o seguinte: Logs de erros SQL, Exibições individuais de detalhes de bancos de dados, Status de agente SQL, Resultados de trabalhos, Fragmentação de índices, Conexões de SQL Server;
6.4.55.9.25. Deve fornecer monitoramento aprofundado (AppInsight) de servidores de função de caixa de correio do Microsoft Exchange, incluindo desempenho do repositório de informações, banco de dados, armazenamento, replicação etc.;
6.4.55.9.26. Deve analisar as tendências de e-mails e anexos enviados e recebidos de cada usuário de caixa de correio;
6.4.55.9.27. Deve fornecer monitoramento aprofundado (AppInsight) do Microsoft Internet Information Service (IIS), incluindo serviços, processos, conexões com sites individuais e tempo de resposta, pool de aplicativos individuais e outras estatísticas, como cache e conexão.;
6.4.55.9.28. Deve fornecer monitoramento aprofundado de produtos do Microsoft Office 365, incluindo Caixas de correio do Exchange, tráfego de e-mail, segurança, status de assinaturas e estatísticas de dispositivos móveis;
6.4.55.9.29. A solução de gerenciamento proposta deve fornecer uma interface gráfica de usuário de alta qualidade;
6.4.55.9.30. Deve fornecer uma exibição unificada de alertas, interceptações, eventos etc. em uma única página;
6.4.55.9.31. Deve realçar rapidamente aplicativos com problemas, com base em diferentes propriedades, como:
6.4.55.9.31.1. aplicativos inativos;
6.4.55.9.31.2. aplicativos com problemas;
6.4.55.9.31.3. parâmetros com alta utilização de CPU;
6.4.55.9.31.4. memória, etc;
6.4.55.9.32. Deve permitir a criação de painéis personalizados e exibições restritas para usuários com base em aplicativos (ou seja, seu acesso deve ser baseado em funções);
6.4.55.9.33. Deve permitir a elaboração interativa de gráficos;
6.4.55.9.34. Deve integrar-se ao Active Directory para fins de login de usuários;
6.4.55.9.35. Deve ter opções de integração para visualizar automaticamente objetos relevantes da infraestrutura virtual, como repositórios de dados e objetos de armazenamento,
como LUNs;
6.4.55.9.36. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O resultado deve ser exportável em um formato tabular;
6.4.55.9.37. Criação de relatórios avançada;
6.4.55.9.38. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;
6.4.55.9.39. Deve ser capaz de gerar/criar o relatório via console Web;

6.4.55.9.40. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;
6.4.55.9.41. Deve permitir a personalização de relatórios pela adição/remoção de colunas, definição de filtros, especificação de períodos de tempo, agrupamento de colunas etc.;
6.4.55.9.42. Deve permitir a personalização avançada pelo fornecimento de opções para inserir consultas personalizadas diretas ao banco de dados;
6.4.55.9.43. Deve ter opções para salvar os relatórios personalizados de forma permanente e disponibilizá-los no console Web;
6.4.55.9.44. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;
6.4.55.9.45. Deve permitir o envio por e-mail de painéis criados no console Web;
6.4.55.9.46. Deve ser capaz de configurar tanto gráficos quanto tabelas em um único relatório;
6.4.55.9.47. Deve ter opções para importar/exportar relatórios criados por outros usuários;
6.4.55.9.48. Deve dar suporte a vários formatos, como PDF, HTML e CSV;
6.4.55.9.49. A solução de monitoramento proposta deve ser capaz de gerenciar e exibir eventos/alertas no console Web;
6.4.55.9.50. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;
6.4.55.9.51. O mecanismo de emissão de alertas deve permitir que condições complexas e grupos de condições sejam especificados para restringir a condição do alerta;
6.4.55.9.52. Deve permitir a inserção de consultas personalizadas para criar regras a serem aplicadas ao banco de dados;
6.4.55.9.53. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;
6.4.55.9.54. Deve permitir a criação de alertas com base em estados sustentados;
6.4.55.9.55. Deve ter diversas ações que possam ser tomadas, incluindo, entre outras, envio de e-mails, encaminhamento de interceptações de SNMP, execução de arquivos executáveis, envio de alertas de texto por SMS, reprodução de sons, envio de uma página da
Web por e-mail etc.;
6.4.55.9.56. Deve ter suporte a variáveis na mensagem de e-mail de alerta para tornar o conteúdo mais autoexplicativo;
6.4.55.9.57. A solução de monitoramento proposta deve permitir o agrupamento de aplicativos segundo diversas propriedades:
6.4.55.9.57.1. por departamento;
6.4.55.9.57.2. por local;
6.4.55.9.57.3. por nome;
6.4.55.9.57.4. e por outras propriedades coletadas;
6.4.55.9.58. Deve permitir a adição dinâmica de membros a grupos pela especificação de uma propriedade capaz de alterar valores dinamicamente, como volumes que estejam ficando
com pouco espaço livre;
6.4.55.9.59. Deve ser capaz de definir relacionamentos entre servidores e aplicativos para evitar alertas de falso positivo por e-mail em caso de interrupção;

6.4.55.9.60. A solução de monitoramento proposta deve ser capaz de representar os aplicativos pictoricamente e exibir detalhes de desempenho de aplicativos em tempo real;
6.4.55.9.61. Deve permitir a personalização de planos de fundo, ícones etc. e deve permitir que vários mapas sejam aninhados com recurso de busca detalhada;
6.4.55.9.62. A solução de monitoramento proposta não deve ser específica a um aplicativo;
6.4.55.9.63. Os aplicativos descobertos devem ser monitorados com modelos de monitoramento incorporados criados com base em práticas recomendadas;
6.4.55.9.64. A solução de monitoramento proposta deve permitir a inclusão de scripts personalizados para estender os recursos de monitoramento dos aplicativos;
6.4.55.9.65. Deve ser capaz de obter, em tempo real, valores, gráficos e alertas dessas propriedades personalizadas;
6.4.55.9.66. Deve ter APIs disponíveis para importar/exportar nós programaticamente e executar funcionalidades semelhantes;
6.4.55.9.67. Deve ter utilitários para exibir o banco de dados e para interromper e iniciar serviços de aplicativos;
6.4.55.9.68. Deve ter exibições móveis personalizadas do console para visualização imediata por administradores;
6.4.55.9.69. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;
6.4.55.9.70. Deve integrar-se ao software de monitoramento de virtualização para oferecer uma exibição do desempenho do aplicativo de ponta a ponta, desde o aplicativo até a VM e o
host.;
6.4.55.9.71. Deve permitir a integração com aplicativos de terceiros na camada de interface do usuário, por meio de troca de mensagens e também de APIs;
6.4.55.9.72. A solução de monitoramento proposta deve ser capaz de acomodar o crescimento pela adição de aplicativos de balanceamento de carga;
6.4.55.9.73. Deve permitir que informações de várias instâncias do aplicativo sejam consolidadas em uma única exibição;
6.4.55.10. Monitoramento de virtualização:
6.4.55.10.1. A solução de monitoramento proposta deve ser capaz de fazer o gerenciamento de hipervisores heterogêneos, como ambientes VMware vSphere e Microsoft
Hyper-V, em um único local;
6.4.55.10.2. Deve fazer o monitoramento do desempenho de ambientes VMware, incluindo VMware ESX, vSphere, ESXi, vCenter Server;
6.4.55.10.3. Deve coletar informações de desempenho e capacidade de clusters, hosts e máquinas virtuais (VMs) no armazenamento do Hyper-V;
6.4.55.10.4. Deve fazer o monitoramento de desempenho e indicar problemas, como problemas de E/S de armazenamento;
6.4.55.10.5. Deve monitorar, detectar e solucionar problemas proativamente de afunilamentos de capacidade;
6.4.55.10.6. Deve possibilitar cenários hipotéticos e ajudar a determinar o posicionamento ideal de VMs;

6.4.55.10.7. Deve ajudar a planejar novas compras e identificar recursos super e subutilizados;
6.4.55.10.8. Deve ajudar a controlar a dispersão de VMs com análise avançada;
6.4.55.10.9. Deve descobrir VMs ociosas/obsoletas, VMs zumbis, arquivos órfãos e VMs sobrecarregadas;
6.4.55.10.10. Deve ser capaz de rastrear configurações de VMs e hosts ao longo do tempo e mostrar alterações à configuração ambiental;
6.4.55.10.11. Deve permitir a comparação de configurações ao longo do tempo e ajudar a ver
exatamente quando uma configuração foi alterada, para ajudar acelerando e melhorando a solução de problemas;
6.4.55.10.12. Deve possibilitar a automação de estorno, identificar custos de nuvem e exibir showback;
6.4.55.10.13. Deverá possuir recursos de planejamento de capacidade, onde:
6.4.55.10.13.1. Fornece um assistente de cenário que ajuda a criar modelos de configuração de VMs e simula o cenário com base no histórico de desempenho, nas novas necessidades do
sistema e nos recursos atualmente disponíveis;
6.4.55.10.13.2. Fornece recomendações preditivas para recursos de CPU, memória e armazenamento que usam padrões e tendências históricas;
6.4.55.10.13.3. Gera um relatório com estatísticas detalhadas de uso que abrangem consumo
previsto de recursos e recomendações para atendimento de necessidades futuras;
6.4.55.10.13.4. Deve ser capaz de executar correções imediatamente ou em lotes, de acordo com a programação, com os dados fornecidos pelas recomendações automáticas;
6.4.55.10.14. Deve ser capaz de descobrir e monitorar instâncias EC2 na nuvem via API;
6.4.55.10.15. Deve ser capaz de descobrir e monitorar volumes EBS na nuvem via API;
6.4.55.10.16. Deve ser capaz de descobrir e monitorar o serviço de nuvem via API;
6.4.55.10.17. Deve ser capaz de descobrir e monitorar novas instâncias automaticamente;
6.4.55.10.18. Deve fornecer uma exibição consolidada de sistemas em nuvem, híbridos e locais;
6.4.55.10.19. A solução de gerenciamento proposta deve fornecer uma interface gráfica de usuário de alta qualidade;
6.4.55.10.20. Deve permitir a personalização por contar com opções para adicionar/remover widgets em página da Web, conforme necessário;
6.4.55.10.21. Deve permitir a criação de painéis personalizados para diferentes finalidades, como painéis separados para monitoramento de desempenho, planejamento de capacidade,
estorno etc.;
6.4.55.10.22. Deve ter opções de integração para visualizar automaticamente aplicativos relevantes e objetos de armazenamento, como LUNs, e integrá-los a objetos de infraestrutura
virtual relevantes, como repositórios de dados e clusters;
6.4.55.10.23. Deve fornecer um painel dinâmico que possibilite visibilidade aprofundada e correlacione pontos de dados históricos díspares em diferentes partes da infraestrutura. O

resultado deve ser exportável em um formato tabular;
6.4.55.10.24. Deve fornecer uma interface para executar a correção em um único clique de problemas de recursos de VMs;
6.4.55.10.25. A solução de monitoramento proposta deve fornecer relatórios atuais e históricos prontos para uso de diversas estatísticas monitoradas;
6.4.55.10.26. Deve ser capaz de gerar relatórios estatísticos que possam ser usados como referência para futuro planejamento ou solução de problemas;
6.4.55.10.27. Deve permitir que os relatórios sejam enviados de acordo com programações diárias, semanais e mensais;
6.4.55.10.28. Deve permitir o envio por e-mail de painéis criados no console Web;
6.4.55.10.29. A solução de monitoramento proposta deve ajudar a detectar rapidamente e tratar problemas de desempenho usando alertas flexíveis e recomendações integradas;
6.4.55.10.30. A solução de monitoramento proposta deve ser capaz de exibir eventos e alertas no console Web;
6.4.55.10.31. As informações de alertas e eventos devem ser registradas no banco de dados para referência futura;
6.4.55.10.32. Deve permitir a criação de novos alertas a partir do zero, bem como de limites personalizáveis;
6.4.55.10.33. A solução de monitoramento proposta deve permitir o agrupamento de dispositivos segundo diversas propriedades:
6.4.55.10.33.1. por departamento;
6.4.55.10.33.2. por local;
6.4.55.10.33.3. por nome;
6.4.55.10.33.4. e por outras propriedades coletadas;
6.4.55.10.34. Deve ter recursos de pesquisa avançada para pesquisar, filtrar e classificar segundo os atributos de configuração e desempenho coletados;
6.4.55.10.35. Deve ser capaz de exibir relacionamentos entre recursos conectados ao longo do tempo para mapear as dependências entre os objetos do datacenter virtual, como VMs, hosts, repositórios de dados, clusters e vApps;
6.4.55.10.36. Deve ser capaz de obter propriedades de virtualização e personalizá-las em exibições de painéis por meio de recursos de pesquisa avançada;
6.4.55.10.37. Deve ser instalável em um ambiente VMware ou Hyper-V, devendo exigir apenas uma instalação para gerenciar um ambiente VMware e Hyper-V misto;
6.4.55.10.38. Deve integrar-se ao software de monitoramento de aplicativos para oferecer uma exibição do desempenho do aplicativo de ponta a ponta, desde o aplicativo até a VM e o
host.;
6.4.55.10.39. Deve ajudar a identificar se o aplicativo está apresentando problemas devido à
VM onde reside ou devido a outras VMs com alto consumo de recursos no mesmo recurso compartilhado;
6.4.55.10.40. Deve ser capaz de integrar-se a módulos que atendem a outras finalidades de monitoramento e fornecer uma exibição centralizada;
6.4.55.10.41. A solução de monitoramento proposta deve ser capaz de monitorar ambientes distribuídos em larga escala com mais de 10.000 VMs;

6.4.56. A solução deverá atender as métricas mínimas listadas abaixo:
6.4.56.1. Equipamentos de rede Links: Firewalls/Switches/WI-FI:
6.4.56.1.1. Consumo do Link;
6.4.56.1.2. Throughput;
6.4.56.1.3. Latência do Link;
6.4.56.1.4. Consumo de Processador;
6.4.56.1.5. Disponibilidade;
6.4.56.1.6. Consumo de memória;
6.4.56.1.7. Disponibilidade.
6.4.56.2. Servidores Físicos: VMWARE Infraestrutura: Datastores/FileIT:
6.4.56.2.1. Espaço em Disco;
6.4.56.2.2. Consumo de memória;
6.4.56.2.3. Consumo de discos;
6.4.56.2.4. Consumo de processador;
6.4.56.2.5. Espaço livre de discos;
6.4.56.2.6. Disponibilidade;
6.4.56.2.7. Taxas de crescimento;
6.4.56.2.8. Capacidade e distribuição de hosts;
6.4.56.2.9. VMs em snapshot;
6.4.56.3. Storages:
6.4.56.3.1. Consumo de processador;
6.4.56.3.2. Utilização das controladoras;
6.4.56.3.3. Utilização e saúde dos discos;
6.4.56.3.4. Disponibilidade;
6.4.56.4. Integração com solução de ITSM para abertura de tickets automática e encerramento automático;
6.4.56.5. Servidores virtualizados e não virtualizados - Gestão de Falhas, Desempenho e Mudança:
6.4.56.5.1. VMware vCenter 1 para Servidores e VMWare VCenter 3 para Desktops;
6.4.56.5.2. Active Directory R2-2012;
6.4.56.5.3. Status dos serviços;
6.4.56.5.4. DNS Server e DHCP Server;
6.4.56.5.5. DFS Replication;
6.4.56.5.6. Kerberos Key Distribution Center;
6.4.56.5.7. Windows Time;
6.4.56.5.8. DNS Client;
6.4.56.5.9. Security Accounts Manager;
6.4.56.5.10. Server;
6.4.56.5.11. Workstation;
6.4.56.5.12. Remote Procedure Call;
6.4.56.5.13. Net Logon;
6.4.56.5.14. Active Directory Domain Services;
6.4.56.5.15. Contadores de LDAP;
6.4.56.5.16. Sessão em uso;
6.4.56.5.17. Tempo de pesquisa LDAP;

6.4.56.5.18. Quantidade de pesquisa por tempo;
6.4.56.5.19. Bloqueio de conta
6.4.56.6. Monitoração de arquivos:
6.4.56.6.1. Alteração do conteúdo do arquivo;
6.4.56.6.2. Quantidade de arquivos em uma pasta;
6.4.56.6.3. Existência de um arquivo ou pasta;
6.4.56.6.4. Tamanho do arquivo e tamanho da pasta;
6.4.56.6.5. Análise de arquivos de LOG;
6.4.56.6.6. Localizar uma determinada String dentro de um arquivo de LOG;
6.4.56.7. Aplicação de Atualização do Windows e/ou aplicação instalada:
6.4.56.7.1. Indicar última vez que foi instalado uma atualização Windows; e/ou
6.4.56.7.2. aplicação e se houve reinicialização do servidor;
6.4.56.8. Event Viewer:
6.4.56.8.1. Indicar um alerta/falha de aplicação;
6.4.56.8.2. Indicar logon e logout;
6.4.56.8.3. Indicar shutdown e restart com qual usuário;
6.4.56.9. Análise de Performance de Rede de Dados:
6.4.56.9.1. Deverá suportar banco de dados relacional para permitir a extração dos dados por ferramentas de terceiros;
6.4.56.9.2. Deverá permitir expansões futuras ao software adquirido acrescentando maior capacidade de dispositivos a serem monitorados;
6.4.56.9.3. A solução não deverá depender para a execução das funções descritas neste documento da instalação de agentes nos ativos monitorados;
6.4.56.9.4. Deverá possuir arquitetura para escalar a solução para quantidades maiores do que previstas neste documento, sendo possível balancear a carga da monitoração em diferentes sondas ou elementos, mantendo a administração única e sem custos adicionais além das licenças adicionais;
6.4.56.9.5. Deverá suportar nativamente a análise das comunicações IPv4 e IPv6 através da coleta de dados dos ativos de rede nos formatos NetFlow e sFlow compatíveis com os ativos de rede da CONTRATANTE;
6.4.56.9.6. A licença contratada para o quantitativo descrito neste documento deverá suportar o uso de “flows” para todos os ativos existentes na infraestrutura da CONTRATANTE;
6.4.56.10. Infraestrutura – requisitos gerais:
6.4.56.10.1. Deverá suportar nativamente a coleta de dados com o uso dos protocolos SNMPv2 e SNMPv3. (get e trap), WMI, ICMP e agentes proprietários;
6.4.56.10.2. Deverá permitir de forma nativa receber traps SNMP e tratá-las através da execução de ações pela solução;
6.4.56.10.3. A solução deve ser capaz de importar e monitorar MIBs de SNMP proprietárias;
6.4.56.10.4. Deverá possuir a capacidade para autodescobrimento da rede, sendo fornecidos apenas os endereços das sub-redes e comunidade SNMP;
6.4.56.10.5. A solução deverá montar de forma automática uma topologia visual dos elementos de conectividade descobertos e inventariados, apresentando os ativos de rede com
suas respectivas conexões, utilizando os protocolos LLDP ou CDP;

6.4.56.10.6. A solução deverá permitir identificar os protocolos citados a partir da análise das comunicações de qualquer ativo de rede monitorado;
6.4.56.10.7. Deverá emitir alertas e possibilitar nativamente a execução de rotinas automáticas em caso de mudanças do cenário normal. As ações possíveis devem permitir a reinicialização de serviços, executar programas externos ou comandos em CLI (Command Line
Interface) diretamente no sistema operacional hospedeiro da solução;
6.4.56.10.8. Deve permitir que os dados estatísticos gerados sejam exportados em formatos HTML, PDF e CSV contendo imagens e análises da ferramenta para auxílio a resolução de problema;
6.4.56.10.9. Permitir a inserção de comentários e/ou textos descritivos em elementos monitorados;
6.4.56.11. Infraestrutura – Agentes:
6.4.56.11.1. Possuir coleta de métricas, livre de instalação de agentes, fazendo uso de SNMP, WMI e outros protocolos;
6.4.56.11.2. Possibilitar a execução de scripts nas máquinas monitoradas, sem o uso de agentes, fazendo uso de protocolos como SSH e Telnet;
6.4.56.11.3. Permitir que agentes, se usados, operem em forma passiva (o controlador inicia a comunicação) e ativa (realiza a comunicação em intervalo de tempo determinado, independente do controlador);
6.4.56.11.4. Usar criptografia na comunicação entre agentes e o controlador;
6.4.56.12. Infraestrutura - Gestão de Falhas e Desempenho de Rede:
6.4.56.12.1. Monitorar e analisar em tempo real, em profundidade, as estatísticas de desempenho de rede para quaisquer dispositivos habilitados para SNMP nas versões v1, v2 e
v3, WMI e SSH;
6.4.56.12.2. Efetuar inventário dos ativos de rede indicando a conectividade entre os dispositivos, ou seja, deve ser capaz de listar qual dispositivo está conectado em cada uma de
suas portas, permitindo traçar mapas de rede, sendo que estes mapas poderão ser customizados pelo usuário;
6.4.56.12.3. Deve possuir no mínimo as seguintes informações:
6.4.56.12.3.1. Nome do dispositivo;
6.4.56.12.3.2. Endereço IP;
6.4.56.12.3.3. Nome da porta;
6.4.56.12.3.4. Dispositivo conectado;
6.4.56.13. A ferramenta deve efetuar inventário dos switches e roteadores da rede indicando:
6.4.56.13.1. O número total de portas e o status de utilização de cada uma delas;
6.4.56.13.2. Status de utilização de vLans, indicando quais switches, roteadores e quais portas fazem parte de determinada vLan;
6.4.56.13.3. vLans configuradas, incluindo seus switches e roteadores;
6.4.56.13.4. Quais dispositivos fazem parte de determinada sub-rede;
6.4.56.14. O inventário deve conter no mínimo as seguintes informações através de coletas automáticas:

6.4.56.14.1. Categoria;
6.4.56.14.2. Descrição;
6.4.56.14.3. Tipo de dispositivo;
6.4.56.14.4. Versão do firmware;
6.4.56.14.5. Versão do hardware;
6.4.56.14.6. Endereço IP;
6.4.56.14.7. Localização;
6.4.56.14.8. MAC Address;
6.4.56.14.9. Modelo;
6.4.56.14.10. SNMP OID;
6.4.56.14.11. Número de série;
6.4.56.14.12. Service Tag;
6.4.56.14.13. Fabricante;
6.4.56.14.14. Informações de garantia do equipamento;
6.4.56.14.15. EOS;
6.4.56.15. Fornecer dados históricos para fins de planejamento de capacidade, com armazenamento por período mínimo de um ano;
6.4.56.16. Fornecer informações sobre interrupções ou inoperâncias por meio de cores e /ou formato de ícones, informando se os elementos estão ou não ativos, e se os parâmetros estão ou não dentro dos limites preestabelecidos pelo fabricante;
6.4.56.17. Realizar descobrimento automático da topologia de nível 2 e nível 3 da rede para apresentação do mapa de conectividade e de informações de configurações dos elementos;
6.4.56.17.1. O descobrimento de nível 2 deverá suportar pelo menos os seguintes métodos de pesquisa:
6.4.56.17.1.1. Consulta a tabelas ARP;
6.4.56.17.1.2. Consulta a tabelas de endereços IP;
6.4.56.17.1.3. Consulta a tabelas de roteamento;
6.4.56.17.1.4. Consulta a informações de Spanning Tree.
6.4.56.18. Acompanhar o desempenho dos links contratados e VPN em tempo real; via Probe devido à falta de acesso SNMP nos routers das operadoras e via interface do dispositivo
de rede interno;
6.4.56.19. Permitir a criação de grupos de dispositivos, interfaces ou grupos parametrizáveis e análise de disponibilidade deles;
6.4.56.20. Permitir a correlação de eventos através da criação de dependências entre grupos parametrizáveis e dispositivos de rede;
6.4.56.21. Habilitar alertas para eventos correlacionados, condições mantidas e combinações complexas de estados de dispositivos. Devendo incluir no mínimo:
6.4.56.21.1. Causa da falha;
6.4.56.21.2. Severidade;
6.4.56.21.3. Hora de início e fim;
6.4.56.21.4. Descrição do dispositivo;
6.4.56.21.5. Endereço IP.
6.4.56.22. As notificações devem suportar no mínimo os seguintes formatos:

6.4.56.22.1. E-mail;
6.4.56.22.2. SNMP Traps;
6.4.56.23. As notificações devem permitir no mínimo a execução das seguintes ações:
6.4.56.23.1. Execução de aplicações externas;
6.4.56.23.2. Mensagens de Syslog;
6.4.56.23.3. Execução de scripts;
6.4.56.23.4. Start e restart de serviços;
6.4.56.24. Permitir a categorização dos ativos de rede por geolocalização, ou departamento, assim como a criação de novas categorias para a classificação deles.
6.4.56.25. Permitir acréscimo de monitoramentos personalizados através da inclusão de MIB's no sistema.
6.4.56.26. Conter mecanismos ou ferramentas inclusas de MIB Walker, MIB Explorer e Gerenciador de MIB's SNMP.
6.4.56.27. Possuir um centro de mensagens único para todos os alertas de eventos em dispositivos e/ou serviços de maneira a permitir correlação desses eventos.
6.4.56.28. Permitir a configuração ou agendamento de descobrimento automático na rede.
6.4.56.29. Permitir a criação de relatórios de rede personalizados, que possam ser impressos ou visualizados na interface web, e exportados para os formatos PDF e planilhas eletrônicas compatíveis com o Microsoft Office 365 e superiores;
6.4.56.30. Permitir adição de mapas gráficos escolhendo entre vários modelos integrados geograficamente ou importar imagem lógica da rede.
6.4.56.31. Deve possibilitar a consulta de tabela das interfaces de rede, incluindo nome, velocidade, status, tráfego de entrada e saída e erros de entrada e saída, assim como descartes de pacotes nas interfaces;
6.4.56.32. Deve possibilitar a consulta de informações da tabela ARP, tanto IPV4 quanto IPV6.
6.4.56.33. Deve possibilitar a consulta da tabela de roteamento, tanto IPV4, quanto IPV6.
6.4.56.34. Deve possibilitar consultas as informações de desempenho do sistema gerenciado, incluindo:
6.4.56.34.1. Utilização de partições de disco, em valor absoluto e percentual;
6.4.56.34.2. Estatísticas dos discos físicos (input e output), incluindo quantidade de leituras e escritas;
6.4.56.34.3. Tabela de processos incluindo ID do processo, memória usada, tamanho, tempo de CPU, horário de início, processo pai e número de threads;
6.4.56.34.4. Tabela dos principais processos do sistema.
6.4.56.34.5. Ferramenta deve ser capaz de executar análise em tempo real possibilitando:
6.4.56.34.5.1. Selecionar um grupo de dispositivos e consultar uma variável do dispositivo a intervalos regulares de tempo e colocar os valores em gráficos;
6.4.56.34.5.2. Selecionar um grupo de variáveis de um dispositivo e consultar o seu valor a intervalos regulares de tempo e colocar esses valores em gráficos;
6.4.56.34.5.3. Incluir os valores em um único gráfico ou em vários gráficos;
6.4.56.34.5.4. Obter informação histórica pelo menos 1 hora antes de iniciar a análise em tempo real;
6.4.56.34.5.5. Gravar estes perfis de análise em tempo real para o seu uso posterior.
6.4.56.35. Linux:

6.4.56.35.1. CPU Usado, em Idle;
6.4.56.35.2. CPU em espera de I/O;
6.4.56.35.3. Fila de processos para execução;
6.4.56.35.4. Interrupção por segundo;
6.4.56.35.5. Disco – Tempo de leitura de cache;
6.4.56.35.6. Espaço por partição;
6.4.56.35.7. Leitura e escrita de blocos por segundo;
6.4.56.35.8. Memória RAM Total;
6.4.56.35.9. Memória RAM usada;
6.4.56.35.10. Uso de SWAP;
6.4.56.35.11. Espaço total de SWAP;
6.4.56.35.12. Processos Zumbi;
6.4.56.35.13. Número de processos com um determinado nome;
6.4.56.36. Windows Server 2003, 2008, 2012 incluindo o R2, 2016, 2019 e superior:
6.4.56.36.1. Status dos servicos;
6.4.56.36.2. Distributed Transaction Coordinator;
6.4.56.36.3. Security Accounts Manager;
6.4.56.36.4. Remote Registry;
6.4.56.36.5. Plug and Play;
6.4.56.36.6. Total de memória disponível;
6.4.56.36.7. % de memória em uso;
6.4.56.36.8. Tamanho do arquivo de SWAP usado;
6.4.56.36.9. Uso em % dos processadores;
6.4.56.36.10. Número de páginas escritas ou lidas do disco por segundo;
6.4.56.36.11. Tamanho da fila de requisições para acesso ao disco físico e logico;
6.4.56.36.12. Monitorar Windows Event Log Monitor;
6.4.56.36.13. Espaço nas partições;
6.4.56.36.14. Número de processos com um determinado nome;
6.4.56.36.15. Impacto no host físico, se Windows for virtual, objetivo identificar se existe problema de performance no device físico;
6.4.56.36.16. Quem e quando fez último logon e logoff;
6.4.56.37. Windows Domain Controllers 2012 (Controladores de domínio):
6.4.56.37.1. Número de usuários bloqueados e desabilitados;
6.4.56.37.2. Alerta de usuário bloqueado;
6.4.56.37.3. Número de novas contas criadas;
6.4.56.37.4. Número de tentativas logons de um usuário (ataque de força bruta);
6.4.56.37.5. Alerta de tentativa de logon e falha por senha ou compatibilidade Kerberos;
6.4.56.37.6. Número de contas ativas sem uso por mais de 30 dias;
6.4.56.37.7. Número de alterações na política Kerberos do domínio;
6.4.56.37.8. Alerta de falha Kerberos;
6.4.56.37.9. Número de alterações na política de auditoria do domínio;
6.4.56.37.10. Número de desligamento do servidor;
6.4.56.37.11. Número de alterações na hora do sistema;
6.4.56.37.12. Windows Update (rotina executada pelo Qualys Patch management);
6.4.56.37.13. Número de dias desde a última atualização;

6.4.56.37.14. Alerta de servidor precisando reiniciar para aplicar atualização;
6.4.56.37.15. Alerta indicando se o servidor está instalando atualizações;
6.4.56.38. Windows DHCP Server:
6.4.56.38.1. Número de Pacotes recebido por segundo;
6.4.56.38.2. Número de pacotes duplicados descartados;
6.4.56.38.3. Tamanho da fila ativa;
6.4.56.38.4. Requisições por segundo;
6.4.56.38.5. Acks e Nacks por segundo;
6.4.56.38.6. Release (Renovação de ip) por segundo;
6.4.56.38.7. Status do serviço: DHCP Server;
6.4.56.38.8. Alertas em caso de erro no Jet Database;
6.4.56.38.9. Alerta em caso de esgotamento de IP livres em um escopo;
6.4.56.39. Windows DHCP Server:
6.4.56.39.1. Uso de memória do banco de dados do DNS;
6.4.56.39.2. Número de atualizações dinâmicas recebidas e rejeitadas;
6.4.56.39.3. Número de Consultas recursivas por segundo;
6.4.56.39.4. Número de Consultas recursivas que falhou por segundo;
6.4.56.39.5. Número de Consultas recursivas que falou por timeout por segundo;
6.4.56.39.6. Status do serviço: DNS Server;
6.4.56.39.7. Número de Consultas recebidas por segundo em TCP e UDP;
6.4.56.39.8. Número de Consultas respondidas por segundo em TCP e UDP;
6.4.56.40. Windows Servidores de Impressão:
6.4.56.40.1. Número de Jobs com erro;
6.4.56.40.2. Número de Jobs no spool;
6.4.56.40.3. Número de Jobs;
6.4.56.40.4. Monitor do serviço: Print Server Spooler;
6.4.56.40.5. Número de Threads do Print Server;
6.4.56.41. Windows Remote Desktop Services Licensing:
6.4.56.41.1. Número de licenças em uso
6.4.56.41.2. Monitora o serviço: Remote Desktop Licensing
6.4.56.41.3. Erros de inicialização no Event sobre serviço de licenciamento.
6.4.56.41.4. Erros de Database no Event sobre serviço de licenciamento.
6.4.56.42. SSL Certificado em servidor WWW
6.4.56.42.1. Verifica se o servidor aceita conexões SSL.
6.4.56.42.2. Verifica a data de expiração do certificado.
6.4.56.43. Internet Information Services (IIS)
6.4.56.43.1. Serviço WEB: Contador de Bytes Recebidos por tempo
6.4.56.43.2. Serviço WEB: Contador de Bytes enviados por tempo
6.4.56.43.3. Serviço WEB: Contador de conexões ativa
6.4.56.43.4. Serviço WEB: Contador de GET por tempo
6.4.56.43.5. Monitor de status do serviço: World Wide Web Publishing
6.4.56.43.6. Testa um formulário básico de autenticação como um usuário.
6.4.56.44. Servidor HTTP
6.4.56.44.1. Monitorar a disponibilidade e tempo de resposta de um servidor externo a infraestrutura da Copel Telecom, em HTTP e HTTPS

6.4.56.45. Oracle Database
6.4.56.45.1. Espaço livre em %
6.4.56.45.2. Espaço usado na Tablespace em %
6.4.56.45.3. Relação de uso do cache de dicionário em relação aos pedidos totais
6.4.56.45.4. Número de usuários conectados
6.4.56.45.5. Tamanho dos arquivos temporários
6.4.56.45.6. Tamanho dos arquivos de dados (Data Files)
6.4.56.45.7. Número de operações de sort que foram executadas completamente na memória
6.4.56.45.8. Número de rollbacks manuais por usuários
6.4.56.46. Citrix Presentation Server e Citrix Metaframe Server
6.4.56.46.1. Citrix IMA Networking: Conexões de rede
6.4.56.46.2. Citrix Licensing: Tempo de resposta (ms) do servidor de licença
6.4.56.46.3. Citrix Licensing: Licença Falha de conexão do servidor
6.4.56.46.4. Citrix sessao ICA: Latency – Last Recorded
6.4.56.46.5. Citrix sessao ICA: Latency – Session Average
6.4.56.46.6. Citrix sessao ICA: Latency – Session Deviation
6.4.56.46.7. Citrix Presentation Server: Número de threads ocupado XML
6.4.56.46.8. Citrix Presentation Server: Número de sessões ativas
6.4.56.46.9. Citrix Presentation Server: Número de sessões desconectadas
6.4.56.46.10. Monitora pelo menos os serviços:
6.4.56.46.11. Citrix Services Manager; Citrix Print Manager Service; Citrix WMI Service; Citrix Licensing (no servitor de Licença);
6.4.56.46.12. Citrix Group Policy Engine e Citrix Licensing Support Service, Citrix MFCOM Service (Metaframe COM Server), Citrix Independent Management Architecture
6.4.56.47. Lotus Domino Server
6.4.56.47.1. Uso de memória e CPU do processo Administrative Process
6.4.56.47.2. Uso de memória e CPU do processo Agent Manager
6.4.56.47.3. Uso de memória e CPU do processo Calendar Connector
6.4.56.47.4. Uso de memória e CPU do processo Event Monitor
6.4.56.47.5. Uso de memória e CPU do processo IMAP Server
6.4.56.47.6. Uso de memória e CPU do processo LDAP Server
6.4.56.47.7. Uso de memória e CPU do processo POP3 Server
6.4.56.47.8. Uso de memória e CPU do processo Replicator
6.4.56.47.9. Uso de memória e CPU do processo Router
6.4.56.47.10. Uso de memória e CPU do processo Schedule Manager
6.4.56.47.11. Uso de memória e CPU do processo Database Server
6.4.56.47.12. Uso de memória e CPU do processo Indexer
6.4.56.47.13. Números de sessões abertas
6.4.56.47.14. Recursos disponíveis em %
6.4.56.47.15. Número de Task LDAP
6.4.56.48. Tomcat Server (JMX)
6.4.56.48.1. Memória livre da heap na JVM
6.4.56.48.2. Memória ocupada da heap na JVM
6.4.56.48.3. Memória máxima da heap na JVM

6.4.56.48.4. Tempo total de processamento do servidor
6.4.56.48.5. Total de Bytes recebido e enviados
6.4.56.48.6. Número de requisições
6.4.56.48.7. Número de erros requisições de processamento
6.4.56.49. VMware ESX Host
6.4.56.49.1. Usando a API do VMware fornece as seguintes métricas:
6.4.56.49.2. CPU Reserved Capacity. Average
6.4.56.49.3. CPU Usage (Average). average
6.4.56.49.4. CPU Usage in MHz (Average). average
6.4.56.49.5. Disk Usage (Average). average
6.4.56.49.6. Memory Active (Average). average
6.4.56.49.7. Memory Balloon (Average). average
6.4.56.49.8. Memory Consumed (Average). average
6.4.56.49.9. Memory Granted (Average). average
6.4.56.49.10. Memory Heap (Average). average
6.4.56.49.11. Memory Heap Free (Average). average
6.4.56.49.12. Memory Overhead (Average). average
6.4.56.49.13. Memory Reserved Capacity. Average
6.4.56.49.14. Memory Shared (Average). Average
6.4.56.49.15. Memory Shared Common (Average). average
6.4.56.49.16. Memory State. Latest
6.4.56.49.17. Memory Swap In (Average). average
6.4.56.49.18. Memory Swap Out (Average). average
6.4.56.49.19. Memory Swap Used (Average). average
6.4.56.49.20. Memory Unreserved (Average). average
6.4.56.49.21. Memory Usage (Average). average
6.4.56.49.22. Memory Used by vmkernel. average
6.4.56.49.23. Memory Zero (Average). average
6.4.56.49.24. Network Usage (Average). average
6.4.56.49.25. System.Uptime. latest
6.4.56.50. VMware vCenter Server
6.4.56.50.1. Uso de CPU e memoria só serviço: VMWare Certificate
6.4.56.50.2. Uso de CPU e memoria só serviço: VMware Directory
6.4.56.50.3. Uso de CPU e memoria só serviço: VMware Kdc
6.4.56.50.4. Uso de CPU e memoria só serviço: VMware vCenter Inventory
6.4.56.50.5. Uso de CPU e memoria só serviço: VMware Virtual Center Management Webservices
6.4.56.50.6. Uso de CPU e memoria só serviço: VMware Virtual Center Server
6.4.56.50.7. Uso de CPU e memoria só serviço: VMware vSphere Web Client
6.4.56.50.8. Testar se o VCenter está pronto para receber conexão nas portas HTTP, HTTPS, LDAP, SSL
6.4.56.51. Infraestrutura – robôs de testes sintéticos
6.4.56.51.1. Monitor que simula o uso de um cliente de DNS onde se mede o tempo de
6.4.56.51.2. resposta do servidor DNS e se as respostas são os endereços esperados
6.4.56.51.3. Monitor que simula que realiza consulta em bancos de dados usando driver

ODBC reportando as métricas de tempo para recebimento dos dados criando
6.4.56.51.4. base estatística para análise de performance.
6.4.56.51.5. Monitor que simula que realiza consulta em bancos de dados ORACLE não fazendo uso de driver ODBC reportando as métricas de tempo para recebimento dos dados criando base estatística para análise de performance.
6.4.56.51.6. Monitor que simula que realiza conexões com servidor FTP realizando autenticação de usuário e download de um arquivo, identificando tempo de download e teste
de integridade deste arquivo.
6.4.56.51.7. Monitor que simule o acesso a uma página web HTTP:
6.4.56.51.8. Identifique a quantidade de bytes recebidos
6.4.56.51.9. Pesquise uma String para verificação do conteúdo
6.4.56.51.10. Retorne o tempo de acesso
6.4.56.51.11. Monitoramento IBM MQ
6.4.56.51.12. Monitoramento de Storage Dell
6.4.56.51.13. Monitoramento de Storage Dell XtremIO

6.5. Da exigência de carta de solidariedade

Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida
pelo fabricante, que assegure a execução do contrato.
6.5.1. Declaração, específica para este certame, emitida pelo fabricante,
comprovando que o licitante está apto e qualificado a vender e comercializar as soluções e os
serviços técnicos objeto deste Termo de Referência. Se a equipe técnica da CONTRATANTE achar necessário, ele poderá realizar diligência para confirmar a veracidade das informações fornecidas;
6.5.1.1. A declaração específica solicitada acima deverá ser apresentada em papel timbrado, original ou cópia reprográfica autenticada, assinado(s) por autoridade ou representante de quem o(s) expediu, com a devida identificação;
6.5.2. A proponente deverá comprovar para os itens de 01 à 07, por meio de
declaração formal emitida pelo fabricante da solução de segurança que é uma revenda autorizada com classificação “GOLD PARTNER” ou “PLATINUM PARTNER”, e que está apta a comercializar e prestar assistência e suporte "on-site" para a solução proposta.
6.5.2.1. A exigência do credenciamento se justifica em razão de que o fornecedor deverá possuir todo o suporte técnico direto com o fabricante do software, evitando possível ausência no fornecimento de suporte ou de atualizações e um quadro de profissionais certificados, visando uma prestação dos serviços de excelência à esta municipalidade;
6.5.2.2. A exigência do credenciamento com a referida classificação se baseia, dentre outros, na relevância da prestação do serviço, que trata de segurança cibernética, que enseja a
prestação de serviço por empresas altamente especializadas capazes de atender demandas de urgência com a devida e necessária efetividade, que é a capacidade de realizar uma demanda (eficácia) da melhor maneira possível (eficiência).

6.6. Subcontratação
Não é admitida a subcontratação do objeto contratual.
É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original, sejam mantidas as demais cláusulas e condições contratuais, não
haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade contratual.
6.7. Requisitos de Experiência Profissional
Os serviços de suporte e garantia referente a solução de segurança, deverão ser prestados por
técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos
ferramentais necessários para a prestação dos serviços;
Comprovação de o licitante possui, em seu quadro de funcionários, na data prevista para a entrega da proposta, profissional de nível superior ou outro devidamente reconhecido pela respectiva entidade profissional competente e que seja certificado pelo fabricante dos produtos
objeto desta licitação. Deverá apresentar a certificação do(s) técnico(s) mediante certificados
emitidos pelo fabricante.
6.8. Requisitos de Formação da Equipe
Para a solução de segurança, os serviços deverão ser prestados por técnicos devidamente capacitados, de acordo com os critérios estabelecidos a seguir:
Consultor em Segurança da Informação:
Atribuições:
Realizar avaliações de riscos para identificar possíveis ameaças aos sistemas de informação e avaliar a probabilidade e o impacto potencial dessas ameaças.
Desenvolver políticas e procedimentos de segurança da informação para mitigar os riscos identificados.
Implementar as políticas e procedimentos de segurança.
Treinar e conscientizar sobre segurança da informação para os membros da organização.
Realizar testes de segurança, como testes de penetração ou "pentests", para identificar quaisquer vulnerabilidades nos sistemas de informação e avaliar a eficácia das medidas de segurança implementadas.
Auxiliar a responder de maneira eficaz, sobre incidentes de segurança ocorridos, investigando o incidente, a mitigação dos danos, a recuperação dos sistemas e dados afetados.
Realizar análise de rastreamento de malware e ataques cibernéticos: identificação, monitoramento e análise de qualquer amostra de malware ativa ou inativa visando a organização, qualquer atividade de botnet passada ou presente e qualquer atividade de rede suspeita.
Trabalhar com indicadores de ameaças de diferentes tipos: Hashes; IP com reputação correspondente; URLs; URLs curinga; URLs contendo scripts com parâmetros

específicos; URLs que cobrem o conteúdo da pasta com subpastas; Domínios e subdomínios.
Trabalhar com a organização para implementar medidas adequadas para proteger os dados pessoais, como criptografia, controles de acesso e sistemas de detecção e resposta a incidentes de segurança.
Proporcionar treinamento e educação para a equipe da organização para garantir que todos compreendam suas responsabilidades em relação à segurança da informação e estejam equipados para cumprir essas responsabilidades.
Auxiliar na resposta contra incidentes, investigando o que aconteceu, avaliando o impacto, notificando as partes afetadas e as autoridades reguladoras conforme necessário.
Ajudar a reconhecer a melhor maneira de prevenir um ataque contra a organização, identificar rotas e informações disponíveis para um invasor, identificar vetores de ameaças, alvos potenciais para ataques, identificar vazamento de informações e monitoramento de fóruns e comunidades online clandestinas.

Formação Acadêmica Necessária:

Diploma de graduação em curso de nível superior em Graduação em Administração, Ciência da Computação ou Engenharia, devidamente registrado, fornecido por instituição de ensino superior reconhecida pelo Ministério da Educação.

Experiência:

Mínima de 5 anos.

Certificações Obrigatórias:

Certificação de solução segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets.
Certificação de solução de incidentes de cibersegurança complexos utilizando recursos exclusivos de detecção e resposta estendidos.
Certificação de solução de segurança para Mail Gateway.
Certificação de solução de segurança para Microsoft Office 365.
Certificação de solução de segurança para ambientes virtualizados.
Certificação de solução de Cyber Threat Intelligence (Inteligência de Ameaças Cibernéticas).
Certificação de solução de segurança para servidores.
Certificação de solução em Combate à Fraude e Compliance.
Certificação de solução de Data Loss Prevention (prevenção de perda de dados).

7. Estimativa da demanda - quantidade de bens e serviços

Diante das análises qualitativa e quantitativa realizadas ao longo do presente estudo técnico preliminar, constata-se que, para fins de um processo de contratação de licenças de software,
se faz necessário o seguinte volume de licenças seja atendido:

LOTE ÚNICO				
ITEM	ESPECIFICAÇÃO	CATMAT	UNIDADE DE MEDIDA	QTDE

1	Software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets com detecção e resposta e software de AntiSpam/proteção para o Microsoft office 365	27456	Unidade	3.200
2	Software de segurança e antivírus para ambientes virtualizados on premise	27456	Unidade por processador	180
3	Software de segurança e antivírus para ambientes virtualizados em cloud	27456	Unidade por VM	320
4	Software de segurança e antivírus para ambientes virtualizados em cloud	27456	Unidade por VM	500
5	Software de detecção e resposta gerenciado	27456	Unidade	1
6	Software de segurança para Storage (por pacotes de 500 usuários)	27464	Unidade	8
7	Software de detecção contra-ataques complexos e direcionados	27456	Unidade	1
8	Software de prevenção contra a perda de dados	27456	Unidade	3200
9	Software de monitoramento de aplicações	27456	Unidade	5.000

	e infraestrutura de redes e servidores			
10	Serviços de Instalação e Configuração	27456	Horas Técnicas	400
11	Treinamentos dos Softwares Licenciados	3840	Unidade	20

O processo licitatório se dará por LOTE ÚNICO, visando concentrar em uma única empresa o
fornecimento das licenças, de instalação e configuração e de treinamento. Por se tratar de uma
solução composta por diversos softwares aplicativos, cada um contendo diversas
funcionalidades, é fundamental, para a garantia da qualidade do serviço, que sejam fornecidos
por um mesmo fornecedor, visando otimizar custos, diminuir tempo de instalação e
configuração e reduzir o tempo de atendimento em caso de problemas.

8. Levantamento de soluções

S1 – Soluções Existentes no Portal do Software Público

Solução viável: não
As soluções disponíveis no Portal do Software Público geralmente são genéricas e servem para alguns propósitos específicos, como por exemplo, soluções para áreas-meio. Porém, esta
Secretaria tem uma série de necessidades específicas, das áreas finalísticas, não tendo soluções no Portal de Software Público

S2 – Existência de Software Disponível

Solução viável: não
Buscamos junto ao portal https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-desolucoes-de-tic, a existência de Catálogo de Soluções de TIC contendo acordo de plataforma
similar para este tipo de segmento. Identificamos apenas catálogos para Microsoft, Oracle, IBM, VMware, Red Hat, Adobe, Broadcom e Qlik, mas não para serviços similares.

S3 – Bitdefender para software de segurança

Solução viável: sim
A Bitdefender é uma renomada empresa global de segurança cibernética que oferece soluções
avançadas de proteção contra uma ampla gama de ameaças digitais, incluindo vírus,
ransomware, exploits zero-day e phishing. Utilizando algoritmos de aprendizado de máquina, a

Bitdefender proporciona proteção em tempo real contra malwares desconhecidos, abrangendo
múltiplas plataformas como Windows, macOS, Android e iOS. Além disso, a empresa integra recursos adicionais, como firewall, proteção web, controle parental e VPN, garantindo uma navegação segura e a privacidade dos dados dos usuários. Suas funcionalidades atendem aos
requisitos exigidos.

S4 – Kaspersky para software de segurança

Solução viável: sim
A Kaspersky oferece uma gama abrangente de soluções de segurança projetadas para proteger usuários individuais, pequenas e médias empresas e grandes corporações contra uma
variedade de ameaças cibernéticas. Seus produtos utilizam algoritmos avançados e técnicas de aprendizado de máquina para detectar, prevenir e eliminar malwares, incluindo vírus, worms, trojans e ransomware. Além da proteção básica contra malware, a Kaspersky também
oferece recursos como firewall integrado, proteção de navegação na web, controle parental e
uma VPN segura. A empresa é frequentemente elogiada por sua eficácia em testes independentes, tornando-se uma escolha confiável para muitos em questões de segurança digital. Suas funcionalidades atendem aos requisitos exigidos.

S5 – F-Secure para software de segurança

A F-Secure oferece uma variedade de produtos e serviços, incluindo antivírus, proteção de endpoint, soluções de segurança para redes e serviços de consultoria em cibersegurança. Seus produtos utilizam tecnologias de detecção modernas, incluindo aprendizado de máquina,
para identificar e bloquear ameaças em tempo real. Além da proteção contra malware, a FSecure também oferece recursos como navegação segura, controle parental, gestão de senhas
e VPN para garantir a privacidade online dos usuários. A empresa é reconhecida por sua abordagem proativa à segurança, frequentemente identificando e divulgando novas vulnerabilidades e ameaças à comunidade de segurança. Suas funcionalidades atendem aos requisitos exigidos.

S6 – Trend Micro para software de segurança

Solução viável: sim
A Trend Micro, ajuda a tornar o mundo seguro para a troca de informações digitais. Impulsionada por décadas de experiência em segurança, pesquisa de ameaças globais e inovação contínua, nossa plataforma de cibersegurança protege mais de 500.000 organizações
e mais de 250 milhões de indivíduos em nuvens, redes, dispositivos e endpoints, oferecendo uma variedade de produtos e serviços para proteger organizações contra ameaças

cibernéticas. Alguns dos produtos em destaque incluem: Cloud Security, Segurança de Endpoint, produtos de Nuvem Híbrida e Gestão e Respostas Centralizadas. A plataforma também oferece visibilidade central para uma melhor, mais rápida detecção e resposta e uma
poderosa gama de técnicas avançadas de defesa de ameaças otimizadas para ambientes, como a AWS, a Microsoft e o Google. Suas funcionalidades atendem aos requisitos exigidos.
Para as opções para solução de software de segurança disponíveis no mercado se apresentam em grande quantidade e muitas versões. Para facilitar a escolha, existem entidades internacionais de consultoria que classificam os fabricantes conforme a sua desenvoltura no mercado. Uma dessas entidades é AV-TEST (https://www.av-test.org/en /antivirus/business-windows-client/). No seu portfólio de soluções avaliadas temos fabricantes
como:
SentinelOne; CrowdStrike; VMware; Trend Micro; Microsoft; Kaspersky; Check Point Software
Technologies; WatchGuard; Broadcom (Symantec); Palo Alto Networks; Malwarebytes; Cybereason; Sophos; Cisco; Cynet; FireEye; Absolute; BlackBerry; Panda Security; McAfee; ESET; WithSecure; TEHTRIS; HarfangLab; Fortinet; Heimdal Security; Tanium; OpenText; 1E; Fidelis; Secureworks; IBM (ReaQta); Elastic; CyCraft; SecPod; Minerva Labs; Deep Instinct; Bitdefender; Sequretek; SlashNext; GoSecure; AhnLab ; ContraForce; Ziften; RSA; Digital Guardian.
Os fabricantes listados acima apenas exemplificam a variedades de fornecedores que existe no mercado e refletem a busca realizada no site da A AV-TEST GmbH - um instituto de pesquisa independente para segurança de TI.
Dado a pesquisa apresentada acima, pode-se observar que existem diversas soluções presentes no mercado que possam cumprir, ao menos em partes, os requisitos aqui elencados. Destacam-se as soluções Kaspersky, a solução Bitdefender, a solução F-Secure e a solução Trend Micro. Em sucinta análise, elas demonstram capacidade de atender as demandas desta Secretaria.

9. Análise comparativa de soluções

Requisito	Solução	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	S1		X	
	S2	X		
	S3	X		
	S4	X		
	S5	X		
	S6	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	S1		X	
	S2		X	
	S3		X	
	S4		X	
	S5		X	
	S6		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	S1		X	
	S2		X	
	S3		X	
	S4		X	

	S5		X	
	S6		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	S1		X	
	S2		X	
	S3		X	
	S4		X	
	S5		X	
	S6		X	
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	S1			X
	S2			X
	S3			X
	S4			X
	S5			X
	S6			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	S1			X
	S2			X
	S3			X
	S4			X
	S5			X
	S6			X

Antes de se iniciar propriamente o procedimento de comparação de custos entre as soluções
viáveis, é importante contextualizar o arcabouço normativo relacionado a contratações públicas
de software na administração.
Para as soluções de software para segurança, haverá o estudo de valores usando como

referência base os preços públicos de cada fabricante e compondo-os aos quantitativos
necessários.

9.1. Disponibilidade de solução similar em outro órgão ou entidade da Administração Pública

No âmbito da Administração Pública, o serviço de subscrição de licenças de software de segurança é amplamente utilizado, dada a sua relevância no cenário atual, onde as ameaças cibernéticas são crescentes, diferenciadas e apresentam elevado grau de sofisticação, exigindo dos governos ações efetivas de prevenção e combate às práticas maliciosas no uso de Tecnologia da Informação, por meio de ações transversais, integradoras, interdisciplinares e multi-setoriais. Os diferentes tipos de tecnologia disponíveis no mercado oferecem diversas técnicas e módulos de proteção tornando as opções disponíveis bastante abrangentes. Dessa forma, a pesquisa de preços e de mercado considerou os filtros que inclui-se os termos "Proteção de Endpoints", "antivírus", "segurança" de forma genérica, e as soluções encontradas em contratações em outras entidades da Administração Pública, foram analisadas conforme o contexto e, posteriormente, foram incluídas no item 11 deste ETP - ANÁLISE COMPARATIVA DE CUSTOS (TCO). A Equipe de Planejamento da Contratação realizou pesquisa de mercado para posterior formação da cesta de preços, além de registro das fontes consultadas, como os portais oficiais do Governo Federal, mídias especializadas, contratações similares em outros entes públicos e pesquisa direta com fornecedores da solução, conforme pode-se verificar no item 11 deste estudo preliminar.

12.1. Quanto à Existência de Software Público Brasileiro

A solução objeto deste estudo preliminar não se trata de software público brasileiro e não consta em seus catálogos, pois trata-se de solução privada que consiste em fornecimento de Software de Segurança Avançada, que permite estabelecer soluções de segurança de estações de trabalho, servidores e storages composta por módulos, configurados através de políticas aplicadas através de um console de gerenciamento centralizado, incluindo suporte técnico especializado.

9.3.Necessidades de Adequação do Ambiente do Órgão ou Entidade

Não foram identificadas necessidades de adequação aos ambientes dos órgãos integrantes deste processo para implantação da solução.

13. Registro de soluções consideradas inviáveis

S1 – Soluções Existentes no Portal do Software Público
Solução viável: não
S2 – Existência de Software Disponível
Solução viável: não

14. Análise comparativa de custos (TCO)

A análise comparativa dos custos deve ser realizada somente nas soluções que se mostrarem
viáveis.

A pesquisa de preços foi realizada mediante a utilização dos seguintes parâmetros:

11.1. Painel de Preços, disponível no endereço eletrônico gov.br/painel de preços, desde que
as cotações refiram-se a aquisições ou contratações firmadas no período de até 1 (um) ano anterior à data de divulgação do instrumento convocatório;
11.2. Dados de pesquisa publicada em mídia especializada, de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do
instrumento convocatório, contendo a data e hora de acesso;
11.3. Pesquisa com contratações similares com outros entes públicos.
11.4. Pesquisa direta com fornecedores, mediante solicitação formal de cotação, desde que os
orçamentos considerados estejam compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do instrumento convocatório.

Série de preços coletados:

11.5. Critérios - A pesquisa de preços, sempre que possível, deverão ser observadas as condições comerciais praticadas, incluindo prazos e locais de entrega, instalação e montagem
do bem ou execução do serviço, formas de pagamento, fretes, garantias exigidas, podendo ser
de quaisquer marcas e modelos, desde que atendam às exigências da contratação.

11.6. Parâmetros – Foram realizadas pesquisas de preços no Portal Nacional de Contratações
Públicas - PNCP e/ou Painel de Preços do Governo e Contratações realizadas por outros Entes Públicos. Além das fontes citadas, foram efetuadas coleta de preços em mídias especializadas e sites comerciais de diversos fornecedores de solução de segurança existentes no mercado, bem como consulta direta junto a esses fornecedores.

11.7. Metodologia - A definição do Método matemático aplicado para a definição do valor esti
mado e as Justificativas para a metodologia utilizada, bem com a definição dos valores esti mados para cada item da contratação.

Foi elaborada a pesquisa de preços e anexado ao processo, com a finalidade de comparar os
preços coletados e inseridos em um Mapa Comparativo de Preços, considerando as fontes pesquisadas.

Como parâmetro de comparação de preços, optou-se pela utilização da média aritmética simples dos preços encontrados nas fontes pesquisadas.
Foi adotado a pesquisa direta com fornecedores, mediante solicitação formal de cotação por email sendo considerado 3 cotações, de diferentes fontes para compor o Anexo I – Mapa
Comparativo de Preços

11.8. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE E MAPA COMPARATIVO DOS CÁLCULOS (TCO)

Para fins de avaliação preliminar dos custos a serem produzidos com a contratação de empresa para fornecer o projeto elencado nesse termo de referência adotou-se procedimento
de pesquisa de preço junto aos fornecedores do mercado e foi realizada pesquisa através de
envio de e-mail.
Essa pesquisa foi realizada pelo Departamento de Tecnologia da Informação e anexada ao
processo no Anexo III – Mapa Comparativo de Preços, sendo realizado esforço para consultar
o maior número de fontes possíveis, a fim de que a pesquisa de preço reflita o real comportamento do mercado e seja alcançado orçamento estimativo confiável para avaliação.

15. Descrição da solução de TIC a ser contratada

A Secretaria de Agricultura e Abastecimento do Estado de São Paulo busca contratar uma
solução integrada de segurança cibernética para fortalecer sua infraestrutura de TI e garantir a
proteção de seus dados e informações sensíveis. Esta solução, alinhada com os esforços
desta Pasta para modernizar e otimizar sua gestão e governança de TI, oferecerá proteção
contra uma ampla gama de ameaças digitais, incluindo vírus, ransomware, exploits zero-day,
phishing e outras ameaças online.
Utilizando tecnologias avançadas, como algoritmos de aprendizado de máquina, a solução
proporcionará detecção em tempo real de malwares desconhecidos e emergentes. Além da
proteção básica contra malware, a solução integrará recursos adicionais, como firewall,
proteção de navegação na web, controle parental e VPN. No aspecto de produtividade e

colaboração, a solução incluirá ferramentas que facilitam a comunicação, a produção digital de
conteúdo, a organização e a colaboração entre as equipes, permitindo a Secretaria de Agricultura e Abastecimento operar de forma mais eficiente e coesa.
A solução consiste na contratação de licenças de software de segurança com as características já explicitadas de forma detalhada no item 6.4 – Requisitos da Contratação.
Esta contratação é essencial para que esta Secretaria possa enfrentar eficientemente os
desafios cibernéticos e operacionais atuais e futuros, garantindo a proteção de suas informações, a conformidade legal, a colaboração interna e a excelência operacional.

16. Estimativa de custo total da contratação

Valor (R$): 18.463.471,67

Os custos totais, estimados, para o contrato de 36 (sessenta) meses é de R$ 18.463.471,67
(dezoito milhões, quatrocentos e sessenta e três mil, quatrocentos e setenta e um reais e sessenta e sete centavos)

Por fim, a Equipe de Planejamento da Contratação atesta expressamente que este Estudo
Técnico Preliminar da Contratação atendeu a todas as orientações contidas na Lei 14.133/21,
conforme descrito nos itens anteriores.

17. Justificativa técnica da escolha da solução

Considerando a análise feita nos itens acima, a contratação de solução de segurança com serviços associados e treinamento, é a única alternativa disponível para atender a demanda da
Secretaria de Agricultura e Abastecimento do Estado de São Paulo e demais órgãos ou entidades participantes.

Inteiramos que cada órgão ou entidade participante, é responsável por justificar seu respectivo
quantitativo.

18. Justificativa econômica da escolha da solução

A escolha econômica da solução se justifica em:

Prevenção de Ameaças Cibernéticas: A utilização de um software antivírus eficiente reduz

significativamente o risco de ataques cibernéticos, que podem causar perdas financeiras
consideráveis e comprometer dados sensíveis.

Economia em Custos de Recuperação: O custo de recuperação de dados e sistemas após um
ataque cibernético geralmente é muito alto. Investir em um software antivírus de qualidade é uma
medida preventiva que pode economizar esses custos.

Minimização de Downtime: Ataques de malware podem resultar em paralisações dos sistemas,
afetando a continuidade das operações. A proteção antivírus minimiza esses períodos de
inatividade, garantindo maior produtividade e evitando custos relacionados à interrupção do
trabalho.

19. Benefícios a serem alcançados com a contratação

- Manter a integridade das informações trafegadas entre o <<CLIENTE>> e outras

instituições.

- Maior nível de segurança no armazenamento dos dados institucionais.
- Viabilizar recursos e otimizar sua aplicação para suprir as necessidades de infraestrutura

e tecnologia.

- Assegurar a excelência da infraestrutura e dos serviços de TI com níveis de

desempenho, segurança e disponibilidade adequados à criticidade do negócio.

- Reduzir custos de treinamento em relação aos usuários finais.
- Aumento da eficiência na troca de dados entre os mais diversos dispositivos e sistemas

de informação;

- Maior gerência e controle sobre a segurança dos acessos a informação;
- Melhor priorização dos serviços relacionados ao negócio;
- Redução de atendimentos sobre incidentes de segurança;
- Padronização de sistemas de segurança e seus eventos;
- Redução no tempo de resposta em caso algum incidente de segurança ou violação;
- Rever falhas e riscos de segurança típicos na infraestrutura de TI;
- Encontrar as vulnerabilidades nos recursos expostos;
- Encontrar as vulnerabilidades do sistema operacional, software de terceiros e protocolos

no ambiente interno;

17. Providências a serem Adotadas

A área requisitante, antes do recebimento do objeto contratado, deverá inteirar-se do conteúdo
do empenho e prever instruções de recebimento do material adquirido.
Conferir se todas as exigências contidas no Termo de Referência foram atendidas, solicitando
a imediata substituição, em caso de produtos diversos daquele solicitado. Sendo rejeitados os
produtos que, por qualquer motivo, se revelem inadequados ao fim que se destinam.

18. Declaração de Viabilidade

Esta equipe de planejamento declara viável esta contratação

18.1. Justificativa da Viabilidade

O presente ESTUDO TÉCNICO PRELIMINAR, elaborado pelos integrantes TÉCNICOS da
Coordenadoria de Tecnologia da Informação em nome da Secretaria de Agricultura e Abastecimento e considerando a análise das alternativas de atendimento das necessidades
elencadas pela área requisitante e os demais aspectos normativos, conclui pela VIABILIDADE
DA CONTRATAÇÃO, uma vez considerados os seus potenciais benefícios em termos de
eficácia, eficiência, efetividade, economicidade e segurança, detalhados neste documento.
Esta contratação trata de bens comuns, sendo comumente adquiridos por muitos órgãos
públicos, e de grande oferta pelo mercado, o que garantirá ampla concorrência e, consequentemente, economia a Secretaria de Agricultura.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543,

04 de setembro de 2024

ELIENE SUZANA VEIGA DE LIMA
Equipe de apoio

ROSEANI MORAES PEREIRA

Equipe de apoio

OTTO LUIZ CASTRO NUNES
Área Técnica

ANEXO I.2

Relação do Órgão Gerenciador e dos Participantes

Estimativas de consumo total, do órgão gerenciador e dos órgãos e entidades participantes, conforme distribuições abaixo:

Sendo:

90102 - ESP-COORD. GERAL ADMINIST. - CGA
90107 - ESP-CTO. VIGILANCIA SANITARIA
90110 - ESP-CTO. REFERENCIA E TREINAMENTO-DST/AIDS
90112 - ESP-GABINETE DO COORDENADOR SEC. SAUDE 1
90115 - ESP-DEPTO.REG.SAUDE - DRS-VI BAURU
90117 - ESP-DEPTO.REG.SAUDE - DRS XI PRES.PRUDENTE
90118 - ESP-HOSP.GERAL PREF. MIGUEL GUALDA DE PROMIS
90120 - ESP-HOSP.EST. DR.OSWALDO B. FARIA -MIRANDOPOL
90121 - ESP-HOSP. REGIONAL DE ASSIS
90122 - ESP-HOSP. DR.ODILO A.SIQUEIRA, P.PRUDENTE
90124 - ESP-DEPTO.REG.SAUDE - DRS-V BARRETOS
90125 - ESP-DEPTO.REG.SAUDE - DRS-VIII FRANCA
90126 - ESP-DEPTO.REG.SAUDE DRS-XIII RIB.PRETO
90127 - ESP-DEPTO.REG.SAUDE - DRS-XV SJRPRETO
90129 - ESP-HOSP. STA.TEREZA, RIB.PRETO
90130 - ESP-CTO.ATENCAO INTEGRAL A SAUDE S.RITA
90131 - ESP-DEPTO.REG.SAUDE - DRS-VII CAMPINAS
90132 - ESP-DEPTO.REG.SAUDE - DRS-X PIRACICABA
90135 - ESP-DEPTO.REG.SAUDE DE TAUBATE - DRS-XVII
90138 - ESP-DEPTO.REG.SAUDE - DRS-IV BAIXADA SANTISTA
90139 - ESP-DEPTO.REG.SAUDE - DRS-XVI SOROCABA
90141 - ESP-HOSP. GUILHERME ALVARO, SANTOS
90145 - ESP-CAIS - PROF. CANTIDIO DE MOURA CAMPOS
90146 - ESP-CTO. REABILITACAO DE CASA BRANCA
90154 - ESP-HOSP. GERAL DE VILA NOVA CACHOEIRINHA

90155 - ESP-HOSPITAL GERAL DE TAIPAS
90157 - ESP-HOSP. REGIONAL SUL
90158 - ESP-HOSP.GERAL J.TEIXEIRA DA COSTA, EM GUAIAN
90159 - ESP-HOSP. GERAL S.MATEUS, DR.MANOEL BIFULCO
90160 - ESP-UN. GESTAO ASSIST I-HOSP. HELIOPOLIS
90161 - ESP-UN. GESTAO ASSISTENCIAL II-HOSP. IPIRANGA
90162 - ESP-UN. GESTAO ASSIST.III - HOSP.INF.DARCY VA
90167 - ESP-HOSP. REG. DR.VIVALDO M.SIMOES, OSASCO
90175- ESP-CTO.ESPECIALIZ. REABILIT DR. APC- M. CRUZE
90170 - ESP-CTO.AT.INTEG.SAUDE MENTAL-DR.DAVID C.C.FI
90172 - ESP-CONJUNTO HOSPITALAR DO MANDAQUI-CHM
90177 - ESP-INSTITUTO ADOLFO LUTZ 90180 - ESP-INSTITUTO DE SAUDE
90181 - ESP-INSTITUTO DANTE PAZZANESE DE CARDIOLOGIA
90182 - ESP-INST. LAURO DE SOUZA LIMA, EM BAURU
90183 - ESP-INST. INFECTOLOGIA EMILIO RIBAS
90187 - ESP-INST.PTA DE GERIATRIA E GERONTOLOG.-IPG
90191 - ESP-DEPTO.REG.GRANDE SAO PAULO - DRS-I G.S.P
90193 - ESP-GRUPO DE GERENCIAMENTO ADMINISTRATIVO
90200 - ESP-GRUPO DE RESGATE - GRAU
90203 - ESP-HOSP.EST.ESPEC.REAB.DR.FRANCISCO R.ARANTE
91101 - ESP-FUNDAÇÃO P/REM. POP.CHOPIN TAVARES DE LIM
102401 - ESP-CTO. EST. EDUC. TECNOL. P. SOUZA - CEETEP
131101 - ESP-FUND.INST. TERRAS JOSE G. DA SILVA ITESP
172201 - ESP-INSTIT DE PESOS E MEDIDAS DO EST. S.PAULO
180101 - ESP-GABINETE DO SECRETARIO E ASSES.SEC.S.PUBL
180183 - ESP-DIRETORIA TEC. INFORMACAO E COMUNICACAO
201201 - ESP-FUND.SISTEMA ESTADUAL ANAL.DADOS-SEADE
252101 - ESP-AG.METROPOLITANA DA BAIXADA SANTISTA
252201 - ESP-AG. METROPOLITANA DE CAMPINAS
262101 - ESP-DEP. DE AGUAS E ENERGIA ELETRICA-DAE
373401 - ESP-EMP. METROP.TRANSPORTES URBS DE SP. SA
390105 - ESP-CENTRO ADMINISTRATIVO - PARCERIA INVEST.
392601 - ESP-AG.REG.SERV.PUBL.DELEG.TRANSP.EST.SP.

930515 - ESP-FUNDAÇAO ONCOCENTRO DE SAO PAULO
990141 - ESP-COORDENADORIA DE ADMINISTRACAO
990202 - ESP-FUNDAÇÃO C.A.S.A. - SEDE ADMINISTRAÇÃO
90179 - ESP-INSTITUTO PASTEUR

| | DESCRIÇÃO | U.F | 90182 - ESP-COORD. ADMINISTRA | 90187 - ESP-CTO. VIDA ANIM | 90120 - ESP-FUNDACAO FAMEMA CIA E HOSPITAL | 90122 - ESP-FUNDACAO DO DESENVOLVIMENTO | 90123 - ESP-CENTRO DE REFERENCIA E | 90127 - ESP-FUNDACAO PIO XII - HEMOCENTRO | 90130 - ESP-FUNDACAO PIO XII - HOSPITAL | 90131 - ESP-FUNDACAO PIO XII - HOSPITAL | 90121 - ESP-FUNDACAO FAMEMA HEMATOLOGIA | 90124 - ESP-FUNDACAO PIO XII - HEMOCENTRO | 90126 - ESP-FUNDACAO PIO XII - HOSPITAL | 90136 - ESP-FUNDACAO PIO XII - HOSPITAL | 90137 - ESP-FUNDACAO PIO XII - HOSPITAL | 90129 - ESP-HOSP. ESTADUAL | 90185 - ESP-HOSP. ESTADUAL | 90131 - ESP-FUNDACAO PIO XII - HOSPITAL | 90132 - ESP-FUNDACAO PIO XII - HOSPITAL | 90185 - ESP-HOSP. ESTADUAL | 90139 - ESP-FUNDACAO PIO XII - HOSPITAL | 90139 - ESP-FUNDACAO PIO XII - HOSPITAL | 90141 - ESP-HOSP. | 90185 - FDP-CJAL | 90185 - ESP-CTO. | 90185 - ESP-HOSP. | 90185 - ESP-HOSP. | 90185 - ESP-HOSP. | 90187 - ESP-HOSP. | 90187 - ESP-HOSP. | 90185 - ESP-HOSP. | 90185 - ESP-HOSP. | 90187 - ESP-HOSP. | 90185 - ESP-HOSP. | 90185 - ESP-HOSP. | 90182 - ESP-CTO. | 90185 - ESP-HOSP. | 90179 - ESP-INSTITUTO | 90185 - ESP-HOSP. | 90185 - ESP-HOSP. | 90185 - ESP-HOSP.

Secretaria de Saúde	INST.PTA DE GERIATRIA E GERONTOLOG.-IPG	PRACA PDE.ALEIXO MONTERIO MAFRA, 34	SAO MIGUEL PTA	São Paulo/SP		VALTER DO NASCIMENTO	(11) 2030-4013
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	FUNDAÇÃO P/REM. POP.CHOPIN TAVARES DE LIM	RUA ENDRES, 35	ITAPEGICA	Guarulhos/SP		WILSON DONIZETE APARECIDO DA SILVA	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	HOSP. REGIONAL DE ASSIS	PCA. SYMPHRONIO A. DOS SANTOS, S/N		Assis/SP		MARCELO LUZ	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	CTO.ESPECIALIZ. REABILIT DR. APC-M.CRUZE	RODOVIA ENGENHEIRO CANDIDO REGO CHAVES KM 3,5		Mogi das Cruzes/SP		JOSE EDUARDO SANTANA MARTINS	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
	AG.REG.SERV.PUBL.DELEG.TRANSP.EST.SP	RUA IGUATEMI, 105		São Paulo/SP		EUGENIO CADIOLI GOUVEA	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	INST. LAURO DE SOUZA LIMA, EM BAURU	RODOVIA COM.JOAO RIBEIRO DE BARROS, KM.225/226		Bauru/SP		GUSTAVO HOJAS CARDOSO	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato

CEETEPS	CTO. EST. EDUC. TECNOL. P. SOUZA - CEETEP	RUA DOS ANDRADAS, 140		São Paulo/SP		ALINE MIRANDA DE ALMEIDA	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	UN. GESTAO ASSISTENCIAL II-HOSP. IPIRANGA	AV. NAZARE, 28 -	IPIRANGA	São Paulo/SP		MARCIA LINARES RODRIGUES	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	DEPTO.REG.GRANDE SAO PAULO - DRS-I G.S.P	RUA CONSELHEIRO CRISPINIANO,20		São Paulo/SP		JOSUE CARLOS DA SILVA	(11) 3017-2065
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	GABINETE DO COORDENADOR SEC. SAUDE 1	AV. DR.ARNALDO, 351 - 5.ANDAR - S/504 -	CERQ.CESAR	São Paulo/SP		ALCIDES LEITE DE SOUZA	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	DEPTO.REG.SAUDE - DRS-X PIRACICABA	RUA DO TRABALHO, 602 -	VL. INDEPENDENCIA	Piracicaba/SP		EDSON HERRERA BRAGA	(19) 3437-7451
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	CTO.AT.INTEG.SAUDE MENTAL-DR.DAVID C.C.FI	AV. MIGUEL ESTEFANO, 3030		São Paulo/SP		PATRICIA DE FREITAS MEDEIROS	(11) 5077-7810
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato

Secretaria de Saúde	INSTITUTO DE SAUDE	RUA SANTO ANTONIO, 590	BELA VISTA	São Paulo/SP		JOICE RODRIGUES DE SOUZA VIEIRA	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	HOSP. REG. DR.VIVALDO M.SIMOES, OSASCO	RUA ARI BARROSO, 355	PRES.ALTINO	Osasco/SP		MARCOS JOEL MORAES	(11) 3683-3077
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	HOSP. REGIONAL SUL	RUA GAL.ROBERTO ALVES DE CARVALHO FILHO, 270		São Paulo/SP		GUILHERME GOMES INVERNIZZI	(11) 5694-8291
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	DEPTO.REG.SAUDE - DRS-V BARRETOS	AV. VINTE HUM, 1238		Barretos/SP		IVANA CLEMENTE CASTRO	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	HOSP. GERAL DE VILA NOVA CACHOEIRINHA	AV. DEP.EMILIO CARLOS, 3000		São Paulo/SP		ELTON BERNARDES DE SOUZA	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	HOSP. GERAL S.MATEUS, DR.MANOEL BIFULCO	RUA ANGELO DE CANDIA, 540	SAO MATEUS	São Paulo/SP		ENILSON DANTAS DA SILVA	(110 2014-5211

Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	DEPTO.REG.SAUDE - DRS-VII CAMPINAS	AV. OROZIMBO MAIA, 75		Campinas/SP		TOBIAS DA SILVA OLIVEIRA	(19) 3739-7003
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
SEFAZ	FUND.SISTEMA ESTADUAL ANAL.DADOS-SEADE	AV. PROF.LINEU PRESTES, 913	CIDADE UNIVERSITARIA	São Paulo/SP		SERGIO RICARDO RABELO	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	HOSP.EST.ESPEC.REAB.DR.FRANCISCO R.ARANTE	RODOVIA WALDOMIRO CORREA DE CAMARGO, KM 62.	VILA MARTINS	Itu/SP		ROSANA APARECIDA SOLER DE SOUZA	(11) 4019-9825
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	GRUPO DE GERENCIAMENTO ADMINISTRATIVO	AV. DR. ARNALDO, 351		São Paulo/SP		ANDERSON DE JESUS DIAS	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	DEPTO.REG.SAUDE DE TAUBATE - DRS-XVII	RUA ALCAIDE MOR CAMARGO, 100 -	ALTO DE SAO JOAO	Taubaté/SP		FRANCISCO ISAIAS TOMAS	(12) 3633-4249/ (12) 3625-2335
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	REG.SAUDE - DRS-IV BAIXADA SANTISTA	AV. EPITACIO PESSOA, 415	APARECIDA	Santos/SP		ANTONIA DE CASSIA DA SILVA	(13) 3278-7786

Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	DEPTO.REG.SAUDE DRS-XIII RIB.PRETO	AV. INDEPENDENCIA, 4770		Ribeirão Preto/SP		PAULO ALEXANDRE DOS SANTOS	(16) 3607-4245
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	GRUPO DE RESGATE - GRAU	Praça CLOVIS BEVILACQUA, 421 - 9º ANDAR -	SE	São Paulo/SP		ANTONIO LEONEL DE SOUZA	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	INST. INFECTOLOGIA EMILIO RIBAS	AV. DR.ARNALDO, 165 -	CERQUEIRA CESAR	São Paulo/SP		CESAR AGUSTINHO DA SILVA	(11) 3896-1270
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
SSP	DIRETORIA TEC. INFORMACAO E COMUNICACAO	AV. CRUZEIRO DO SUL, 260		São Paulo/SP		BASILEU LAURINDO GARCIA JUNIOR	(13) 3202-1340
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	HOSP. GUILHERME ALVARO, SANTOS	RUA OSWALDO CRUZ, 197		Santos/SP		CLAUDIO ROBERTO TROTTI JUNIOR	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato

Secretaria de Saúde	DEPTO.REG.SAUDE - DRS-XV SJRPRETO	AV JANIO QUADROS, 150 -	DISTR.IND.ULYSSES DA SILVEIRA GUIMARAES	São José do Rio Preto/SP		SANDRA REGINA TORRES	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Sec. DESENV. URB. E HABITAÇÃO	AG.METROPOLITANA DA BAIXADA SANTISTA	PCA DOS EXPEDICIONARIOS, NA 10 , 11 ANDAR	GONZAGA -	Santos/SP		GEORGE CHARLES BALTHAZAR JUNIOR	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	INSTITUTO ADOLFO LUTZ	AV. DR.ARNALDO, 355		São Paulo/SP		ELIANE EUFRASIA DOS SANTOS MENEZES	(11) 3068-2851
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	DEPTO.REG.SAUDE - DRS-VI BAURU	RUA QUINTINO BOCAIUVA, 5-45		Bauru/SP		MARIA REGINA ROMAO	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	UN. GESTAO ASSIST.III - HOSP.INF.DARCY VA	RUA DR.SERAPHICO DE ASSIS CARVALHO, 34		São Paulo/SP		LUCIANO MELITIO ALVES	(11) 3723-3788
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	HOSP.EST. DR.OSWALDO B. FARIA - MIRANDOPOL	AV. DR.RAUL DA CUNHA BUENO, 585		Mirandópolis/SP		SHAIRA ARROIO DE ARAUJO	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato

Secretaria de Saúde	DEPTO.REG.SAUDE - DRS XI PRES.PRUDENTE	AV. CEL.JOSE SOARES MARCONDES, 2357		Presidente Prudente/SP		ELIANE ISABEL DE MATOS	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	CTO.ATENCAO INTEGRAL A SAUDE S.RITA	AV. PADRE PIO CORSO, 1523		Santa Rita do Passa Quatro/SP		ARIANE CRISTINA BENATO	(19) 3584-8324
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	DEPTO.REG.SAUDE - DRS-VIII FRANCA	AV. WILSON SABIO DE MELLO, 1833 -	POLO INDUSTRIAL	Franca/SP		GABRIELA CARAMORI BARCELOS	(16) 9124-7709/(16) 3713-4316
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Sec. Da Justiça Cidadania	FUNDAÇÃO C.A.S.A. - SEDE ADMINISTRAÇÃO	RUA FLORENCIO DE ABREU, 848 -	LUZ	São Paulo/SP		JULIO CESAR SIGNORINI	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	HOSPITAL GERAL DE TAIPAS	AVENIDA ELISIO TEIXEIRA LEITE 6999		São Paulo/SP		ELIANA FERNANDES DE CASTRO	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	CTO. REFERENCIA E TREINAMENTO-DST/AIDS	RUA SANTA CRUZ, 81		São Paulo/SP		ELISANGELA CRISTINA BRASILIENSE	(11) 5571-1884
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato

Secretaria de Saúde	CONJUNTO HOSPITALAR DO MANDAQUI-CHM	RUA VOLUNTARIOS DA PATRIA, 4301		São Paulo/SP		MONIQUE RODRIGUES GOMES DOS ANJOS	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	CTO. VIGILANCIA SANITARIA	AV. DR. ARNALDO, 351 -	CEQ. CESAR	São Paulo/SP		CRISTIANE DE BRITO	(11) 3065-465 (11) 3065-4813
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	HOSP. STA.TEREZA, RIB.PRETO	AV. ADELMO PERDIZA, 495		Ribeirão Preto/SP		BRUNO PELLICANI NETO	(16) 3919-9095
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
EMTU	EMP. METROP.TRANSPORTES URBS DE SP. SA	RUA BOA VISTA, 170 - 3º ANDAR	CENTRO	São Bernardo do Campo/SP		LETICIA TATSUTA	(11) 4341-1196
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
DAEE	DEP. DE AGUAS E ENERGIA ELETRICA-DAE	RUA BOA VISTA, 170		São Paulo/SP		MARCOS TADEU YAMAMOTO	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	UN. GESTAO ASSIST I-HOSP. HELIOPOLIS	RUA CONEGO XAVIER, 276		São Paulo/SP		MIRIAM GRAVE	(11) 2067-0522
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato

Secretaria de Saúde	INSTITUTO DANTE PAZZANESE DE CARDIOLOGIA	AV. DR.DANTE PAZZANESE, 500 -	VILA MARIANA	São Paulo/SP		JOSE RAIMUNDO TERCEIRO OLIVEIRA JUNIOR	(11) 5085-6436
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	COORD. GERAL ADMINIST. - CGA	AVA DRA ENEAS DE CARVALHO AGUIAR,188		São Paulo/SP		FABIO FRANCISCO DO NASCIMENTO	(11) 3066-8491
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
SSP	GABINETE DO SECRETARIO E ASSES.SEC.S.PUBL	RUA LIBERO BADARO, 39 -	CENTRO	São Paulo/SP		CARLOS HENRIQUE ANTUNES TAPARELLI	(11) 3291-6923
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
IPEM	INSTIT DE PESOS E MEDIDAS DO EST. S.PAULO	RUA SANTA CRUZ, 1922 -	V.MARIANA	São Paulo/SP		GERALDO MARQUES DA SILVA NETO	(11) 3581-2248/ (11) 3888-5220
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	HOSP.GERAL J.TEIXEIRA DA COSTA,EM GUAIAN	AV. MIGUEL ACHIOLE DA FONSECA, 135		São Paulo/SP		ADEVALDO VICENTE DA SILVA	(11) 2551-3300
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
Secretaria de Saúde	FUNDAÇAO ONCOCENTRO DE SAO PAULO	RUA OSCAR FREIRE NR 2396		São Paulo/SP		ANA PAULA MANO GHILARDI	
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato

INVEST	CENTRO ADMINISTRATIVO - PARCERIA INVEST.	RUA IAIA, 126	ITAIM BIBI	São Paulo/SP		JOSE AUGUSTO RODRIGUES BORGES	(11) 3702-8299
Bloco	Unidade	Logradouro, número	Bairro	Cidade/SP	CEP	Responsável	Contato
SEC. AGRICULTURA E ABASTECIMNETO	FUND.INST. TERRAS JOSE G. DA SILVA ITESP	AV. BRIGADEIRO LUIZ ANTONIO, 554		São Paulo/SP		ALFREDO LOPES JUNIOR	(18) 98127-6826

ANEXO II

MINUTA DE TERMO DE CONTRATO
Lei nº 14.133, de 1º de abril de 2021
SERVIÇOS – LICITAÇÃO

GOVERNO DO ESTADO DE SÃO PAULO
SECRETARIA DE AGRICULTURA E ABASTECIMENTO
(Processo Administrativo n° 007.00023837-2024-15)

PROCESSO SEI n.º 007.00023837-2024-15

PREGÃO ELETRÔNICO COADM n.º90006/2024

CONTRATO XXX n.º XX/2024

UASG: XXXXXX / UGE: XXXXXX

CONTRATO ADMINISTRATIVO Nº *...../2024* CELEBRADO ENTRE O **ESTADO DE SÃO PAULO**, POR INTERMÉDIO DA **SECRETARIA DE AGRICULTURA E ABASTECIMENTO,** ATRAVÉS DA EMPRESA _____, TENDO POR OBJETO A **CONSTITUIÇÃO DE SISTEMA DE REGISTRO DE PREÇOS, PARA CONTRATAÇÃO EVENTUAL E FUTURA CONTRATAÇÃO DE LICENÇAS DE SOFTWARE DE SEGURANÇA, INCLUINDO SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E SUPORTE, TREINAMENTO E ATUALIZAÇÃO DO SOFTWARE.**

O Estado de São Paulo por intermédio da POR INTERMÉDIO DA SECRETARIA DE AGRICULTURA E ABASTECIMENTO com sede, com sede na Praça Ramos de Azevedo, na cidade de São Paulo/Estado de São Paulo, inscrita no CNPJ/MF sob o nº 46.384-400/0018-97, neste ato representada pelo xxxx, nomeado(a) pelo(a) [Portaria/_____] nº ....., de ..... de ..... de 20..., publicado(a) no DOE de ..... de ..... de ....., [portador(a) da identificação funcional_____ nº ...../inscrito(a) no CPF sob o nº..... (se ausente identificação funcional individualizada)], no uso da competência conferida pela legislação aplicável, doravante denominado(a) CONTRATANTE, e o(a) ....., inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., doravante designado(a) CONTRATADO, neste ato representado(a) por ..... (nome e função no Contratado), inscrito(a) no CPF sob o nº....., conforme atos constitutivos da fornecedora **OU** procuração apresentada nos autos, tendo em vista o que consta no Processo nº ..... e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais normas da legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico nº ___/2024, mediante as condições a seguir enunciadas, de acordo com as subdivisões subsequentes na forma de cláusulas e respectivos itens que compõem este instrumento.

1. CLÁUSULA PRIMEIRA – OBJETO (art. 92, I e II)

1.1. O objeto do presente instrumento é a contratação de serviços *de licenças de software de segurança, incluindo serviços de instalação, configuração e suporte, treinamento e atualização do software,* conforme detalhamento e especificações técnicas deste instrumento, do Termo de Referência, da proposta do Contratado e demais documentos da contratação constantes do processo administrativo em epígrafe.

9.2. Objeto da contratação:

ITEM	DESCRIÇÃO	CATSER	U.F	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets com detecção e resposta e software de AntiSpam /proteção para o Microsoft office 36	27464	unidade			
2	Software de segurança e antivírus para ambientes virtualizados on premise	27464	unidade			
3	Software de segurança e antivírus para ambientes virtualizados em cloud	27464	unidade			

4	Software de complemento de detecção e resposta para os itens 02 e 03	27464	unidade			
5	Software de detecção e resposta gerenciado	27464	unidade			
6	Software de segurança para Storage	27464	unidade			
7	Software de detecção contra-ataques complexos e direcionados	27464	unidade			
8	Software de prevenção contra a perda de dados	27464	unidade			
9	Software de monitoramento de aplicações e infraestrutura de redes e servidores	27464	unidade			
10	Serviços de Instalação e Configuração	26972	uni. Serviço técnico			
11	Treinamentos dos Softwares Licenciados	3840	unidade			

9.3. O presente Termo de Contrato vincula-se à seguinte documentação, que se considera parte integrante deste instrumento, independentemente de transcrição:

9.3.1. O Termo de Referência;

9.3.2. O Edital da Licitação;

9.3.3. A Proposta do Contratado; e

9.3.4. Eventuais anexos dos documentos supracitados.

9.4. O regime de execução deste contrato é o de *empreitado por preço unitário.*

10. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

10.1. O prazo de vigência da contratação é de 36(trinta e seis) meses, contados da data da assinatura do contratro, prorrogável por até 10 (dez) anos, a critério do Contratante, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

10.1.1. O Contratado poderá se opor à prorrogação de que trata a subdivisão acima, desde que o faça mediante documento escrito, recepcionado pelo Contratante em até 90 (noventa) dias antes do vencimento do contrato ou de cada uma das prorrogações do prazo de vigência.

10.1.2. Dentre outras exigências, a prorrogação de que trata a subdivisão acima é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração e em harmonia com os preços do

mercado, conforme pesquisa a ser realizada à época do aditamento pretendido, permitida a negociação com o Contratado, observando-se, ainda, os seguintes requisitos:

a) Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

b) Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

c) Seja juntada justificativa, por escrito, de que a Administração mantém interesse na realização do serviço;

d) Haja manifestação expressa do Contratado informando o interesse na prorrogação;

e) Seja comprovado que o Contratado mantém as condições iniciais de habilitação.

10.1.3. O Contratado não tem direito subjetivo à prorrogação contratual, e não poderá pleitear qualquer espécie de indenização em razão da não prorrogação do prazo de vigência contratual por conveniência do Contratante.

10.1.4. Eventuais prorrogações de contrato serão formalizadas mediante celebração de termo aditivo, respeitadas as condições prescritas na Lei nº 14.133, de 2021.

10.1.5. Nas eventuais prorrogações contratuais, custos não renováveis já pagos ou amortizados no âmbito da contratação, quando houver, deverão ser eliminados como condição para a prorrogação.

10.1.6. O contrato não poderá ser prorrogado quando o Contratado tiver sido penalizado com as sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

10.1.7. Não obstante o prazo estipulado nesta cláusula, a vigência nos exercícios subsequentes ao da celebração do contrato estará sujeita a condições resolutivas consubstanciadas:

I - na inexistência de recursos aprovados nas respectivas Leis Orçamentárias de cada exercício para atender as respectivas despesas, acarretando a extinção do contrato a partir de sua ocorrência; ou

II - na ausência de vantagem para o Contratante na manutenção do contrato, desde que o Contratante comunique ao Contratado a opção pela extinção do contrato com ao menos 2 (dois) meses de antecedência em relação à próxima data de aniversário do contrato, acarretando a extinção do contrato a partir da referida data de aniversário contratual.

10.1.8. Ocorrendo a resolução do contrato, com base em uma das condições resolutivas estipuladas na subdivisão acima desta cláusula, o Contratado não terá direito a qualquer espécie de indenização.

11. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (art. 92, IV, VII e XVIII)

11.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de início, conclusão, entrega, observação e recebimento do objeto, e critérios de medição, constam no Termo de Referência, que constitui parte integrante deste Contrato.

12. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

12.1. Não será admitida a subcontratação, cessão ou transferência, total ou parcial, do objeto contratual.

13. CLÁUSULA QUINTA – PREÇO (art. 92, V)

13.1. O valor total da contratação é de R$..... (.....)

13.2. No valor acima estão incluídos, além do lucro, todas as despesas diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

13.3. O valor indicado nesta cláusula é meramente estimativo, de forma que os pagamentos devidos ao Contratado dependerão dos quantitativos efetivamente demandados, medidos e fornecidos.

13.4. Caso o Contratado seja optante pelo Simples Nacional e, por causa superveniente à contratação, perca as condições de enquadramento como microempresa ou empresa de pequeno porte ou, ainda, torne-se impedido de beneficiar-se desse regime tributário diferenciado por incorrer em alguma das vedações previstas na Lei Complementar nº 123, de 2006, não poderá deixar de cumprir as obrigações avençadas perante a Administração, tampouco requerer o reequilíbrio econômico-financeiro, com base na alegação de que a sua proposta levou em consideração as vantagens daquele regime tributário diferenciado.

14. CLÁUSULA SEXTA - PAGAMENTO (art. 92, V e VI)

14.1. O prazo para pagamento ao Contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, que constitui parte integrante deste Contrato.

15. CLÁUSULA SÉTIMA - REAJUSTE (art. 92, V)

15.1. Os preços inicialmente ajustados são fixos e irreajustáveis pelo prazo de 1 (um) ano contado da data do orçamento estimado, que corresponde a __/__/__ (DD/MM/AAAA).

15.2. É previsto reajuste anual dos preços inicialmente ajustados, de modo que, caso o prazo de execução do objeto contratual ultrapasse a data em que se configure 1 (um) ano a contar da data do orçamento estimado, e independentemente de pedido do Contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do índice _____ (indicar o índice a ser adotado), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

15.3. No caso de reajuste(s) subsequente(s) ao primeiro, o interregno mínimo de 1 (um) ano será contado a partir dos efeitos financeiros do último reajuste.

15.4. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

15.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

15.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

15.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

15.8. O reajuste será realizado por apostilamento.

16. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (art. 92, X, XI e XIV)

16.1. São obrigações do Contratante:

16.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e a documentação que o integra;

16.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

16.1.3. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, a expensas do Contratado;

16.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

16.1.5. Comunicar ao Contratado para emissão de Nota Fiscal em relação à parcela incontroversa, para efeito de liquidação e pagamento, se houver parcela incontroversa no caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, observando-se o art. 143 da Lei nº 14.133, de 2021;

16.1.6. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

16.1.7. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

16.1.8. Cientificar o órgão de representação judicial da Procuradoria Geral do Estado para adoção das medidas cabíveis quando necessária medida judicial diante do descumprimento de obrigações pelo Contratado;

16.1.9. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, observado o prazo de *XX (XXX)* para decisão, a contar da conclusão da instrução do requerimento, admitida a prorrogação motivada, por igual período, e excepcionada a hipótese de disposição legal ou cláusula contratual que estabeleça prazo específico;

16.1.10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo Contratado no prazo máximo de *10 (dez)dias*, contado a partir da conclusão da instrução do requerimento, sendo admitida a prorrogação motivada desse prazo por igual período, e observado o disposto no parágrafo único do artigo 131 da Lei nº 14.133, de 2021;

16.1.11. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais;

16.1.12. Comunicar ao Contratado na hipótese de posterior alteração do projeto pelo Contratante, se o caso estiver enquadrado na situação disciplinada pelo art. 93, § 3º, da Lei nº 14.133, de 2021.

16.1.13. Observar, no tratamento de dados pessoais de profissionais, empregados, prepostos, administradores e/ou sócios do Contratado, a que tenha acesso durante a execução do objeto a que se refere a cláusula primeira deste contrato, as normas legais e regulamentares aplicáveis, em especial, a Lei nº 13.709, de 14 de agosto de 2018, com suas alterações subsequentes.

16.2. O prazo para resposta ao pedido de restabelecimento do equilíbrio econômico-financeiro não se iniciará enquanto o Contratado não cumprir os atos ou apresentar a documentação solicitada pelo Contratante para adequada instrução do requerimento.

16.3. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus profissionais, prepostos ou subordinados.

17. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO (art. 92, XIV, XVI e XVII)

17.1. O Contratado deve cumprir todas as obrigações estabelecidas em lei, e aquelas constantes deste Contrato e da documentação que o integra, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

17.1.1. Designar e manter preposto aceito pelo Contratante para representar o Contratado na execução do contrato;

• A indicação ou a manutenção do preposto do Contratado poderá ser recusada pelo Contratante, desde que devidamente justificada, hipótese em que o Contratado deverá designar outro para o exercício da atividade;

17.1.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II, da Lei nº 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados;

17.1.3. Alocar os profissionais necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, utilizando os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e à legislação de regência;

17.1.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

17.1.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado diretamente à Administração ou a terceiros em razão da execução do contrato, não excluindo nem reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida na documentação que integra este instrumento, o valor correspondente aos danos sofridos;

17.1.6. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do Contratante, de agente público que desempenhe(ou) função na licitação ou de fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

17.1.7. Quando não for possível a verificação da regularidade no Sistema de Cadastramento Unificado de Fornecedores – Sicaf ou em outros meios eletrônicos hábeis de informações, o Contratado deverá atender a notificação para entregar ao setor responsável pela fiscalização do contrato, no prazo de 5 (cinco) dias úteis, os seguintes documentos: 1) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 2) certidões que comprovem regularidade fiscal perante as Fazendas Estadual/Distrital e/ou Municipal/Distrital do domicílio ou sede do Contratado que tenham sido exigidas para fins de habilitação na documentação que integra este instrumento; 3) Certidão de

Regularidade do FGTS – CRF; e 4) Certidão Negativa, ou positiva com efeitos de negativa, de Débitos Trabalhistas – CNDT;

17.1.8. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, ou Dissídio Coletivo de Trabalho das categorias abrangidas pelo contrato, e por todas as obrigações e encargos trabalhistas, previdenciários, fiscais, sociais, comerciais e os demais previstos em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante, nos termos do artigo 121 da Lei nº 14.133, de 2021;

17.1.9. Comunicar ao Fiscal do contrato, assim que possível, qualquer ocorrência anormal ou acidente que se verifique no local da execução dos serviços;

17.1.10. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do objeto;

17.1.11. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;

17.1.12. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato;

17.1.13. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina;

17.1.14. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do Termo de Referência, observando-se o disposto no Capítulo VII do Título III da Lei nº 14.133, de 2021;

17.1.15. Não permitir a utilização de qualquer trabalho do menor de 16 (dezesseis) anos, exceto na condição de aprendiz para os maiores de 14 (quatorze) anos, nem permitir a utilização do trabalho do menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre;

17.1.16. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

17.1.17. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas (art. 116 da Lei nº 14.133, de 2021);

17.1.18. Comprovar o cumprimento da reserva de cargos a que se refere a subdivisão acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei nº 14.133, de 2021);

17.1.19. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato, respondendo, administrativa, civil e criminalmente por sua indevida divulgação e incorreta ou inadequada utilização;

17.1.20. Arcar com o ônus decorrente de eventual equívoco no dimensionamento de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros, mas que sejam previsíveis em seu ramo de atividade;

17.1.21. Cumprir as disposições legais e regulamentares federais, estaduais e municipais que interfiram na execução do objeto, bem como as normas de segurança do Contratante;

17.1.22. Realizar os serviços de manutenção e assistência técnica no(s) seguinte(s) local(is) ... [inserir endereço(s)];

- O técnico deverá se deslocar ao local da repartição, salvo se o Contratado tiver unidade de prestação de serviços em distância de até [....] [inserir distância conforme avaliação técnica] do local demandado.

17.1.23. Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo ser exigida do Contratado, inclusive, a capacitação dos técnicos do Contratante ou do novo fornecedor que continuará a execução dos serviços;

17.1.24. Ceder ao Contratante todos os direitos patrimoniais relativos ao objeto contratado, o qual poderá ser livremente utilizado e/ou alterado em outras ocasiões, sem necessidade de nova autorização do Contratado.

- Considerando que o objeto da contratação envolve a elaboração de projeto relativo a obra imaterial de caráter tecnológico, insuscetível de privilégio, a cessão de todos os direitos patrimoniais a que se refere a subdivisão anterior inclui o fornecimento de todos os dados, documentos e elementos de informação pertinentes à tecnologia de concepção, desenvolvimento, fixação em suporte físico de qualquer natureza e aplicação da obra, nos termos do § 1º do art. 93 da Lei nº 14.133, de 2021.

17.2. Em atendimento à Lei nº 12.846, de 2013, e ao Decreto estadual nº 67.301, de 2022, o Contratado se compromete a conduzir os seus negócios de forma a coibir fraudes, corrupção e quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira, de modo que o Contratado não poderá oferecer, dar ou se comprometer a dar a quem quer que seja, tampouco aceitar ou se comprometer a aceitar de quem quer que seja, por conta própria ou por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios de qualquer espécie relacionados de forma direta ou indireta ao objeto deste contrato, o que deve ser observado, ainda, pelos seus prepostos, colaboradores e eventuais subcontratados, caso permitida a subcontratação.

17.2.1. O descumprimento das obrigações previstas na subdivisão acima poderá submeter o Contratado à extinção unilateral do contrato, a critério do Contratante, sem prejuízo da aplicação das sanções penais e administrativas cabíveis e, também, da instauração do processo administrativo de responsabilização de que tratam a Lei nº 12.846, de 2013, e o Decreto estadual nº 67.301, de 2022.

17.3. O Contratado obriga-se a não admitir a participação, na execução deste contrato, de:

17.3.1. agente público de órgão ou entidade licitante ou contratante, ou terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica, nos termos dos §§ 1º e 2º do artigo 9º da Lei nº 14.133, de 2021;

17.3.2. pessoa que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, nos termos do inciso IV do artigo 14 e/ou parágrafo único do artigo 48 da Lei nº 14.133, de 2021;

17.3.3. pessoas que se enquadrem nas demais vedações previstas no artigo 14 da Lei nº 14.133, de 2021.

18. CLÁUSULA DÉCIMA - OBRIGAÇÕES PERTINENTES À LGPD

18.1. No âmbito da execução do objeto deste contrato, o Contratado deve cumprir a Lei nº 13.709, de 14 de agosto de 2018, com suas alterações subsequentes (Lei Geral de Proteção de Dados Pessoais - LGPD), as demais normas legais e regulamentares aplicáveis à proteção de dados pessoais, inclusive regulamentos editados pela Autoridade Nacional de Proteção de Dados, e deve observar as instruções por escrito do Contratante no tratamento de dados pessoais.

18.1.1. O Contratado deve assegurar que o acesso a dados pessoais seja limitado aos empregados, prepostos ou colaboradores que necessitem conhecer/acessar os dados pertinentes, na medida em que sejam estritamente necessários para as finalidades deste contrato, e cumprir a legislação aplicável, assegurando que todos esses indivíduos estejam sujeitos a compromissos de confidencialidade ou obrigações profissionais de confidencialidade.

18.1.2. Considerando a natureza dos dados tratados, as características específicas do tratamento e o estado atual da tecnologia, assim como os princípios previstos no caput do artigo 6º da Lei nº 13.709, de 2018, o Contratado deve adotar, em relação aos dados pessoais, medidas de segurança, técnicas e administrativas aptas a proteger os dados e informações de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

18.1.3. Considerando a natureza do tratamento, o Contratado deve, enquanto operador de dados pessoais, implementar medidas técnicas e organizacionais apropriadas para o cumprimento das obrigações do Contratante previstas na Lei nº 13.709, de 2018.

18.1.4. O Contratado deve:

• notificar o Contratante na primeira oportunidade possível, ao receber requerimento de um titular de dados, na forma prevista no artigo 18 da Lei nº 13.709, de 2018; e

• quando for o caso, auxiliar o Contratante na elaboração da resposta ao requerimento a que se refere a subdivisão anterior.

18.1.5. O Contratado deve notificar ao Contratante, na primeira oportunidade possível, a ocorrência de incidente de segurança relacionado a dados pessoais, fornecendo informações suficientes para que o Contratante cumpra quaisquer obrigações de comunicar à autoridade nacional e aos titulares dos dados a ocorrência do incidente de segurança sujeita à Lei nº 13.709, de 2018.

18.1.6. O Contratado deve adotar as medidas cabíveis para auxiliar na investigação, mitigação e reparação de cada um dos incidentes de segurança.

18.1.7. O Contratado deve auxiliar o Contratante na elaboração de relatórios de impacto à proteção de dados pessoais, observado o disposto no artigo 38 da Lei nº 13.709, de 2018, no âmbito da execução deste Contrato.

18.1.8. Na ocasião do encerramento deste contrato, o Contratado deve, imediatamente, ou, mediante justificativa, em até 10 (dez) dias úteis da data de seu encerramento, devolver todos os dados pessoais ao Contratante ou eliminá-los, conforme decisão do Contratante, inclusive eventuais cópias de dados pessoais tratados no âmbito deste contrato, certificando por escrito, ao Contratante, o cumprimento desta obrigação.

18.1.9. O Contratado deve colocar à disposição do Contratante, conforme solicitado, toda informação necessária para demonstrar o cumprimento do disposto nesta cláusula, e deve permitir auditorias e contribuir com elas, incluindo inspeções, pelo Contratante ou auditor por ele indicado, em relação ao tratamento de dados pessoais.

18.1.10. O Contratado responderá por quaisquer danos, perdas ou prejuízos causados ao Contratante ou a terceiros decorrentes do descumprimento da Lei nº 13.709, de 2018 ou de instruções do Contratante relacionadas a este contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização do Contratante em seu acompanhamento.

18.1.11. Caso o objeto da presente contratação envolva o tratamento de dados pessoais com fundamento no consentimento do titular de que trata o inciso I do artigo 7º da Lei nº 13.709, de 2018, deverão ser observadas pelo Contratado ao longo de toda a

vigência do contrato todas as obrigações específicas vinculadas a essa hipótese legal de tratamento de dados pessoais, conforme instruções por escrito do Contratante.

18.1.12. É vedada a transferência de dados pessoais, pelo Contratado, para fora do território do Brasil sem o prévio consentimento, por escrito, do Contratante, e demonstração da observância, pelo Contratado, da adequada proteção desses dados, cabendo ao Contratado o cumprimento de toda a legislação de proteção de dados ou de privacidade nacional e de outro(s) país(es) que for aplicável.

18.1.13. O Contratado não poderá realizar subcontratação, tampouco divulgar dados pessoais a qualquer subcontratado, ou substituir subcontratado, exceto se previamente autorizada de forma específica e por escrito pelo Contratante.

18.1.14. O Contratado deve tomar medidas razoáveis para assegurar que empregados, prepostos ou colaboradores de qualquer subcontratado que necessitem conhecer/acessar dados pessoais relacionados à execução deste contrato estejam sujeitos a compromissos de confidencialidade ou obrigações profissionais de confidencialidade, e cumprir, no tocante à subcontratação, todas as disposições aplicáveis da Lei nº 13.709, de 2018.

18.1.15. A subcontratação, mesmo quando autorizada pelo Contratante, não exime o Contratado das obrigações decorrentes deste contrato, de modo que o Contratado permanecerá por elas integralmente responsável perante o Contratante, inclusive na hipótese de descumprimento dessas obrigações por subcontratado.

19. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO (art. 92, XII)

19.1. Não haverá exigência de garantia contratual da execução.

20. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

20.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

20.2. Garantida a prévia defesa, serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

i) **Advertência**, se o Contratado der causa à inexecução parcial do contrato, quando não se justificar a imposição de penalidade mais grave (art. 156, § 2º, da Lei nº 14.133, de 2021);

ii) **Impedimento de licitar e contratar**, se praticadas as condutas descritas nas alíneas "b", "c" e "d" da subdivisão anterior desta cláusula, quando não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii) **Declaração de inidoneidade para licitar ou contratar**, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" da subdivisão anterior desta cláusula, bem como nas alíneas "b", "c" e "d" da referida subdivisão, que justifiquem a imposição de penalidade mais grave (art. 156, § 5º, da Lei nº 14.133, de 2021).

iv) **Multa:**

20.3. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial.

20.4. Para as infrações previstas nos itens 12.1.1, 12.1.2 e 12.1.3, a multa será de 10% (dez por cento) do valor do contrato licitado.

20.5. A multa poderá ser aplicada cumulativamente com as demais sanções previstas neste Contrato (art. 156, § 7º, da Lei nº 14.133, de 2021).

20.5.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157 da Lei nº 14.133, de 2021)

20.5.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada, caso exigida na documentação que integra este instrumento, ou, quando for o caso, será cobrada judicialmente (art. 156, § 8º, da Lei nº 14.133, de 2021).

20.6. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, § 9º, da Lei nº 14.133, de 2021).

20.7. A multa poderá ser aplicada cumulativamente com as demais sanções previstas neste Contrato (art. 156, § 7º, da Lei nº 14.133, de 2021).

20.7.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157 da Lei nº 14.133, de 2021).

20.7.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada, caso exigida na documentação que integra este instrumento, ou, quando for o caso, será cobrada judicialmente (art. 156, § 8º, da Lei nº 14.133, de 2021).

20.8. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no *caput* e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

20.9. Na aplicação das sanções serão considerados (art. 156, § 1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o Contratante;

e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

20.10. As sanções são autônomas e a aplicação de uma não exclui a de outra.

20.11. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159 da Lei nº 14.133, de 2021).

20.12. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos na Lei nº 14.133, de 2021, ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160 da Lei nº 14.133, de 2021).

20.13. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal (Art. 161 da Lei nº 14.133, de 2021).

20.14. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

21. CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

21.1. O contrato poderá ser extinto na forma, pelos motivos e com as consequências previstos nos artigos 137 a 139 e 155 a 163 da Lei nº 14.133, de 2021.

21.1.1. O Contratado reconhece desde já os direitos do Contratante nos casos de extinção por ato unilateral da Administração, prevista no artigo 138 da Lei nº 14.133, de 2021*, bem como no art. 1º, § 2º, item 3, do Decreto estadual nº 55.938, de 2010, com a redação que lhe foi dada pelo Decreto estadual nº 57.159, de 2011, na hipótese da configuração de trabalho em caráter não eventual por pessoas físicas, com relação de subordinação ou dependência, quando o Contratado for sociedade cooperativa (se admitida a participação/contratação de cooperativa)*.

21.1.2. O contrato poderá ser extinto por algum dos motivos previstos no artigo 137 da Lei nº 14.133, de 2021, devendo a extinção ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa.

21.1.3. A alteração social ou modificação da finalidade ou da estrutura da empresa não ensejará a extinção contratual se não restringir sua capacidade de concluir o contrato.

• Se a operação societária de que trata a subdivisão acima implicar mudança em pessoa jurídica contratada, deverá ser formalizada alteração subjetiva por termo aditivo.

21.2. O termo de extinção, sempre que possível, será precedido da indicação de:

21.2.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

21.2.2. Relação dos pagamentos já efetuados e ainda devidos;

21.2.3. Indenizações e multas.

21.3. A extinção do contrato não configura óbice para o reconhecimento de eventual desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, *caput,* da Lei n.º 14.133, de 2021).

21.4. Se for constatada irregularidade no procedimento licitatório ou na execução contratual, caso não seja possível o saneamento, a decisão pelo Contratante sobre a suspensão da execução ou sobre a declaração de nulidade do contrato somente será

adotada na hipótese em que se revelar medida de interesse público, observado o disposto nos artigos 147 a 149 da Lei nº 14.133, de 2021, conferindo-se ao Contratado oportunidade para prévia manifestação e participação na instrução.

22. CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA (art. 92, VIII)

22.1. No presente exercício, as despesas decorrentes desta contratação correrão à conta de recursos específicos consignados no respectivo Orçamento do Estado, na dotação abaixo discriminada:

I. Gestão/Unidade: (a ser definido na contratação);

II. Fonte de Recursos: (a ser definido na contratação);

III. Programa de Trabalho: (a ser definido na contratação);

IV. Elemento de Despesa: (a ser definido na contratação);

V. Plano Interno: (a ser definido na contratação);

VI. Nota de Empenho: (a ser definido na contratação);

22.2. Quando a execução do contrato ultrapassar o presente exercício, a dotação relativa ao(s) exercício(s) financeiro(s) subsequente(s) será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

23. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS (art. 92, III)

23.1. Aplicam-se aos casos omissos as disposições contidas na Lei nº 14.133, de 2021, e disposições regulamentares pertinentes, e, subsidiariamente, as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e princípios gerais dos contratos.

24. CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

24.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

24.2. O Contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários no objeto, a critério exclusivo do Contratante, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

24.3. Se o contrato não contemplar preços unitários para serviços cujo aditamento se fizer necessário, esses serão fixados por meio da aplicação da relação geral entre os valores da proposta e o do orçamento-base da Administração sobre os preços referenciais ou de mercado vigentes na data do aditamento, respeitados os limites estabelecidos no artigo 125 da Lei nº 14.133, de 2021.

24.4. Eventuais alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, respeitadas as disposições da Lei nº 14.133, de 2021, admitindo-se que, nos casos de justificada necessidade de antecipação de seus efeitos, a formalização do aditivo ocorra no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

24.5. Caso haja alteração unilateral do contrato que aumente ou diminua os encargos do Contratado, o equilíbrio econômico-financeiro inicial será restabelecido no mesmo termo aditivo.

24.6. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

25. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

25.1. Incumbirá ao Contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput,* da Lei n.º 14.133, de 2021, e ao art. 8º, § 2º, da Lei n. 12.527, de 2011, c/c art. 22 do Decreto estadual nº 68.155, de 2023.

26. CLÁUSULA DÉCIMA OITAVA– FORO (art. 92, §1º)

26.1. Fica eleito o Foro da Comarca da Capital do Estado de São Paulo para dirimir quaisquer questões que decorrerem deste Termo de Contrato, que não puderem ser resolvidas na esfera administrativa, conforme art. 92, § 1º, da Lei nº 14.133, de 2021.

E assim, por estarem as partes justas e contratadas, foi lavrado o presente instrumento em *01 (uma) via*, que, lido e achado conforme pelo Contratado e pelo Contratante, vai por eles assinado para que produza todos os efeitos de Direito, sendo assinado também pelas testemunhas abaixo identificadas.

[Local], [dia] de [mês] de [ano]. **OU**[Local],

data da última assinatura eletrônica das partes.

_____

Representante legal do CONTRATANTE

_____

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

2-

ANEXO LC-01 - TERMO DE CIÊNCIA E DE NOTIFICAÇÃO (CONTRATOS)

CONTRATANTE:	
CONTRATADO:	
CONTRATO Nº (DE ORIGEM):	
OBJETO:	
ADVOGADO (S)/ Nº OAB/email: (*)	

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

a) o ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;

b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;

c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;

d) as informações pessoais dos responsáveis pela contratante estão cadastradas no módulo eletrônico do "Cadastro Corporativo TCESP – CadTCESP", nos termos previstos no Artigo 2º das Instruções nº01/2020, conforme "Declaração(ões) de Atualização Cadastral" anexa (s);

e) é de exclusiva responsabilidade do contratado manter seus dados sempre atualizados.

2. Damo-nos por NOTIFICADOS para:

a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;

b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

São Paulo, XX de XXXX de 2024.

AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:

Nome:	Guilherme Piai Silva Filizzola
Cargo:	Secretário de Agricultura
CPF:	401.005.308-93

RESPONSÁVEIS PELA HOMOLOGAÇÃO DO CERTAME:

Nome:	
Cargo:	
CPF:	
Assinatura:	

RESPONSÁVEIS QUE ASSINARAM O AJUSTE:

Pelo Contratante:

Nome:	
Cargo:	
CPF:	
Assinatura:	

Pela Contratada:

Nome:	
Cargo:	
CPF:	
Assinatura:	

ORDENADOR DE DESPESAS DA CONTRATANTE:

Nome:	
Cargo:	
CPF:	
Assinatura:	

(*) Facultativo. Indicar quando já constituído, informando, inclusive, o endereço eletrônico

ANEXO LC-02 - DECLARAÇÃO DE DOCUMENTOS À DISPOSIÇÃO DO TCE-SP

CONTRATANTE:	
CNPJ Nº:	
CONTRATADA:	
CNPJ Nº:	
CONTRATO N° (DE	
DATA DA ASSINATURA:	
VIGÊNCIA:	
OBJETO:	
VALOR (R$):	

Em se tratando de obras/serviços de engenharia:

Declaro, na qualidade de responsável pela entidade supra epigrafada, sob as penas da Lei, que os demais documentos originais, atinentes à correspondente licitação, em especial, os a seguir relacionados, encontram-se no respectivo processo administrativo arquivado na origem à disposição do Tribunal de Contas do Estado de São Paulo, e serão remetidos quando requisitados:

a) memorial descritivo dos trabalhos e respectivo cronograma físico-financeiro;

b) orçamento detalhado em planilhas que expressem a composição de todos os seus custos unitários;

c) previsão de recursos orçamentários que assegurem o pagamento das obrigações decorrentes de obras ou serviços a serem executados no exercício financeiro em curso, de acordo com o respectivo cronograma;

d) comprovação no Plano Plurianual de que o produto das obras ou serviços foi contemplado em suas metas;

e) as plantas e projetos de engenharia e arquitetura.

São Paulo, XX de XXXX de 2024.

RESPONSÁVEL:
Nome:
Cargo:
E-mail institucional:
Assinatura:

ANEXO PC-02 - CADASTRO DO RESPONSÁVEL

ÓRGÃO OU ENTIDADE:

Nome:	
Cargo:	
CPF:	
Período de gestão:	

Obs: 1. Todos os campos são de preenchimento obrigatório.

2. Repetir o quadro, se necessário, informando todos os responsáveis durante o exercício.

3. Anexar a "Declaração de Atualização Cadastral" emitida pelo sistema "Cadastro Corporativo TCESP – CadTCESP", por ocasião da remessa do presente documento ao TCESP.

As informações pessoais dos responsáveis estão cadastradas no módulo eletrônico do Cadastro TCESP, conforme previsto no Artigo 2º das Instruções nº01/2020, conforme "Declaração de Atualização Cadastral" ora anexada (s).

_____

Assinatura do responsável pelo preenchimento

MODELO(S) REFERENTE(S) A PLANILHA DE PROPOSTA

ANEXO *III*

MODELO DE PLANILHA DE PROPOSTA

Contratação de empresa para aquisição de licenças de software de segurança, incluindo serviços de instalação, configuração e suporte, treinamento e atualização do software, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

LOTE ÚNICO						
ITEM	**ESPECIFICAÇÃO**	**CATMAT**	**UNIDADE DE MEDIDA**	**QTDE**	**VALOR UNITÁRIO (R$)**	**VALOR TOTAL (R$)**
01	Software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets com detecção e resposta e software de AntiSpam/proteção para o Microsoft office 365	27456	Unidade	120891		
02	Software de segurança e antivírus para ambientes virtualizados on premise	27456	Unidade por processador	2249		
03	Software de segurança e antivírus para ambientes virtualizados em cloud	27456	Unidade por VM	1649		
04	Software de complemento de detecção e resposta para os itens 02 e 03	27456	Unidade por VM	5621		
05	Software de detecção e resposta gerenciado	27456	Unidade	54067		
06	Software de segurança para Storage	27464	Unidade	769		
07	Software de detecção contra-ataques complexos e direcionados	27456	Unidade	22		
08	Software de prevenção contra a perda de dados	27456	Unidade	58178		

09	Software de monitoramento de aplicações e infraestrutura de redes e servidores	27456	Unidade	40262		
10	Serviços de Instalação e Configuração	26972	Horas Técnicas	5167		
11	Treinamentos dos Softwares Licenciados	3840	Unidade	491		
					VALOR TOTAL (R$)	

ANEXO IV

MODELO(S) DE DECLARAÇÃO(ÕES)

ANEXO IV.1

MODELO DE DECLARAÇÃO EXIGIDA PARA HABILITAÇÃO

(em papel timbrado do licitante)

Eu, _____, portador do CPF nº _____, na condição de representante legal de _____ (nome empresarial ou denominação) , interessado em participar do Pregão Eletrônico nº ___/___, Processo n° ___/___, DECLARO, sob as penas da Lei, que o licitante:

a) cumpre as normas relativas à saúde e segurança no trabalho, nos termos do parágrafo único do artigo 117 da Constituição Estadual; e

b) atenderá, na data da contratação, ao disposto no artigo 5º-C e se compromete a não disponibilizar empregado que incorra na vedação prevista no artigo 5º-D, ambos da Lei nº 6.019, de 1974, com redação dada pela Lei nº 13.467, de 2017, quando o caso.

(Local e data).

_____

(Nome/assinatura do representante legal)

ANEXO IV.2

DECLARAÇÃO DE CONHECIMENTO PLENO DAS CONDIÇÕES E PECULIARIDADES DA CONTRATAÇÃO

(elaborado pelo licitante)

Eu, _____, portador do CPF nº_____, na condição de responsável técnico de _____ (nome empresarial ou denominação), interessado em participar do Pregão Eletrônico nº ___/___, Processo n° ___/___, DECLARO que o licitante tem conhecimento pleno das condições e peculiaridades da contratação, que não realizou a vistoria prévia prevista no Edital e que, mesmo ciente da possibilidade de fazê-la e dos riscos e consequências envolvidos, optou por formular a proposta sem realizar a vistoria prévia que lhe havia sido facultada.

O licitante está ciente desde já que, em conformidade com o estabelecido no Edital, não poderá pleitear em nenhuma hipótese modificações nos preços, prazos ou condições ajustadas, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou informações sobre o(s) local(is) em que será realizado o objeto da licitação.

(Local e data)

_____

(nome/assinatura/qualificação do responsável técnico)

ANEXO V

MINUTA DE ATA DE REGISTRO DE PREÇOS

ATA DE REGISTRO DE PREÇOS

GOVERNO DO ESTADO DE SÃO PAULO
SECRETARIA DE AGRICULTURA E ABASTECIMENTO

N.º ____*/2024*

O **Estado de São Paulo**, por intermédio da **Secretaria de Agricultura e Abastecimento** – **Coordenadoria de Administração**, com sede na Praça Ramos de Azevedo, 254 – Republica – Centro de São Paulo, na cidade de São Paulo, inscrita no CNPJ/MF sob o nº 46.384-400/0018-97, neste ato representada pelo Senhor **RICARDO LORENZINI BASTOS** da Coordenadoria de Administração, nomeado no cargo de Agente de Apoio à Pesquisa Científica e Tecnológica I, Efetivo, conforme art. 20, inciso II, da LC 180/78 - DEC. de 14 - DOE 15/11/08, exercendo as funções em pró-labore de Coordenador, da Coordenadoria de Administração, da Chefia de Gabinete, conforme Diário Oficial de 03/10/2023, inscrito no CPF sob o nº 214.372.518-38, considerando o resultado obtido conforme o processo administrativo n.º 007.00023837/2024-15, resolve celebrar a presente ATA de REGISTRO DE PREÇOS, procedendo ao registro dos preços do(s) fornecedor(es) indicado(s) e qualificado(s) nesta ata, de acordo com a classificação por ele(s) alcançada e na(s) quantidade(s) cotada(s), atendendo às condições previstas no *Edital de licitação*, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, no Decreto estadual nº 67.608, de 27 de março de 2023, c/c o Decreto nº 11.462, de 31 de março de 2023, e demais preceitos da legislação aplicável, e em conformidade com as disposições a seguir, de acordo com as subdivisões na forma de itens que compõem este instrumento.

27. DO OBJETO

27.1. A presente Ata tem por objeto o registro de preços para a eventual contratação de serviços *de licenças de software de segurança, incluindo serviços de instalação, configuração e suporte, treinamento e atualização do software,* conforme o detalhamento e as especificações técnicas constantes da documentação que constitui Anexo do *Edital de*

Pregão Eletrônico nº ...../2024, que é parte integrante desta Ata, assim como as propostas cujos preços tenham sido registrados, independentemente de transcrição.

28. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

28.1. O preço registrado, as especificações do objeto, a quantidade mínima a ser cotada, a quantidade máxima de cada item que poderá ser contratada, fornecedor (es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Fornecedor (razão social, CNPJ/MF, endereço, contatos, representante)						
Item do TR	Especificação	Unidade de Fornecimento	Quantidade	Valor unitário	Valor Total	Prazo
1	Software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets com detecção e resposta e software de AntiSpam /proteção para o Microsoft office 36	Unidade		120891		12 meses
2	Software de segurança e antivírus para ambientes virtualizados on premise	Unidade		2249		12 meses
3	Software de segurança e antivírus para ambientes	Unidade		1649		12 meses

	virtualizados em cloud					
4	Software de complemento de detecção e resposta para os itens 02 e 03	Unidade		5621		12 meses
5	Software de detecção e resposta gerenciado	Unidade		54067		12 meses
6	Software de segurança para Storage	Unidade		769		12 meses
7	Software de detecção contra-ataques complexos e direcionados	Unidade		22		12 meses
8	Software de prevenção contra a perda de dados	Unidade		58178		12 meses
9	Software de monitoramento de aplicações e infraestrutura de redes e servidores	Unidade		40262		12 meses
10	Serviços de Instalação e Configuração	Uni. Serviço técnico		5167		12 meses

11	Treinamentos dos Softwares Licenciados	Unidade		491		12 meses

28.2. A listagem do cadastro de reserva referente ao presente registro de preços consta como anexo desta Ata.

29. ÓRGÃO(S) GERENCIADOR E PARTICIPANTE(S)

29.1. O órgão ou entidade gerenciadora será *Coordenadoria de Tecnologia da informação*

29.2. Além do órgão ou entidade gerenciadora, é(são) órgão(s) ou entidade(s) participante(s) do registro de preços:

Item nº	*Órgão(s) ou Entidade(s) Participante(s)*	*Unidade*	*Quantidade*

30. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

30.1. Durante a vigência desta ata de registro de preços, os órgãos e as entidades da Administração Pública estadual, distrital e municipal que não participaram do procedimento de intenção de registro de preços poderão aderir à ata na condição de não participantes, observados os limites e regras estabelecidos neste instrumento, bem como os seguintes requisitos:

a) apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

b) demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133, de 2021; e

c) *consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.*

30.1.1. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.

O órgão ou entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.

30.1.2. Após a autorização do órgão ou entidade gerenciadora, o órgão ou entidade não participante deverá efetivar a contratação solicitada em até 90 (noventa) dias, observado o prazo de vigência da ata.

30.1.3. O prazo para efetivar a contratação de que trata a subdivisão acima poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou entidade não participante aceita pelo órgão ou entidade gerenciadora, desde que respeitado o limite temporal de vigência da ata de registro de preços.

30.1.4. O órgão ou entidade integrante da ata de registro de preços poderá aderir, na qualidade de não participante, a item(ns) para o(s) qual(is) não tenha quantitativo registrado, observados os requisitos deste item 4.

30.1.5. É da competência do respectivo órgão ou entidade que tenha aderido à ata na condição de não participante, garantidos o contraditório e a ampla defesa, aplicar as penalidades decorrentes do descumprimento das obrigações contratuais, em relação à sua própria contratação, informando as ocorrências ao órgão ou entidade gerenciadora.

Dos limites para as adesões

30.1.6. As contratações adicionais decorrentes das adesões não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o órgão ou entidade gerenciadora e para os participantes.

30.1.7. O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão ou entidade gerenciadora e os participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

31. VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

31.1. O prazo de vigência e validade da Ata de Registro de Preços será de *1 (um) ano, contado a partir do 1º (primeiro) dia útil subsequente à data de divulgação no Portal Nacional de Contratações Públicas (PNCP), podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso*.

31.1.1. A contratação decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e serão observadas, no momento da contratação e a cada exercício financeiro, a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

31.1.2. Na formalização do instrumento da contratação deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

31.2. A formalização da contratação com os fornecedores registrados nesta ata de registro de preços deverá ocorrer no prazo de validade deste instrumento.

31.3. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 2021.

31.4. As contratações respeitarão a ordem de classificação dos fornecedores registrados nesta ata.

31.5. O registro de fornecedores incluído nesta ata na forma de anexo, quando for o caso, consiste na formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

31.6. A fase de apresentação de amostra(s) ou de execução de prova de conceito que seja exigida na documentação que integra o instrumento convocatório, quando houver, e a habilitação dos fornecedores que compõem o cadastro de reserva, quando for o caso, serão efetuadas quando houver necessidade de contratação dos fornecedores remanescentes, por impossibilidade de atendimento da demanda pelo signatário da ata, observada a disciplina estabelecida nesta ata e no instrumento convocatório mencionado no item 1.1.

31.7. O preço registrado, com indicação dos fornecedores, será divulgado no PNCP e ficará disponibilizado durante a vigência desta ata de registro de preços.

31.8. Caso se caracterize hipótese de impossibilidade de atendimento da demanda pelo signatário da ata de que trata o item 5.6, observado o disposto no referido item, ficará facultado à Administração convocar os fornecedores remanescentes do cadastro de reserva, quando houver, na ordem de classificação, para contratação nas condições propostas pelo primeiro classificado.

31.8.1. Na hipótese de nenhum dos fornecedores que aceitaram cotar o objeto com preço igual ao do adjudicatário concordar com a contratação nas condições propostas pelo primeiro classificado nos termos da subdivisão acima, a Administração, observados o valor estimado e sua eventual atualização na forma prevista na documentação que integra o instrumento convocatório mencionado no item 1.1, poderá:

Convocar para negociação os fornecedores remanescentes que mantiveram sua proposta original, quando houver, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário;

Adjudicar e celebrar a contratação nas condições ofertadas pelos fornecedores remanescentes, observado o disposto neste item 5 e a ordem de classificação, quando frustrada a negociação de melhor condição.

31.9. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a contratação pretendida, desde que devidamente justificada.

31.10. No prazo de validade deste instrumento, o(s) órgão(s) ou entidade(s) participante(s) não participará(ão) em outra ata de registro de preços com o mesmo objeto, salvo na hipótese do inciso VIII do *caput* do art. 82 da Lei nº 14.133, de 2021, quando for o caso.

32. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

32.1. Os preços registrados poderão ser alterados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo do(s) item(ns) registrado(s), nas seguintes situações:

a) em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos da alínea “d” do inciso II do *caput* do art. 124 da Lei nº 14.133, de 2021;

b) em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou da superveniência de disposições legais, com comprovada repercussão sobre os preços registrados.

32.2. É previsto reajustamento dos preços registrados nesta ata, observados os mesmos critérios estabelecidos no instrumento convocatório mencionado no item 1.1 para o reajustamento dos preços de eventual contratação dela decorrente.

32.2.1. Caso seja realizado reajustamento dos preços desta ata, somente caberá reajustamento dos preços de eventual contratação dela decorrente se forem observados os requisitos especificados no respectivo instrumento, e for ultrapassado o interregno mínimo de 1 (um) ano contado a partir dos efeitos do reajustamento dos preços desta ata. No caso de reajustamento(s) subsequente(s) ao primeiro, o interregno mínimo de 1 (um) ano será contado a partir dos efeitos do último reajustamento.

Vedação a acréscimo de quantitativos

32.3. É vedado:

a) efetuar acréscimos nos quantitativos fixados nesta ata de registro de preços;

b) *restabelecer os quantitativos que já tenham sido contratados desta ata de registro de preços quando da prorrogação de que trata o item 5.1*.

33. NEGOCIAÇÃO DE PREÇOS REGISTRADOS

33.1. Quando, por motivo superveniente, o preço registrado se tornar superior àquele praticado no mercado, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a sua redução.

33.1.1. Quando for exitosa a negociação a que alude a subdivisão acima, o órgão ou entidade gerenciadora comunicará o novo preço aos órgãos e entidades que tiverem firmado contratos decorrentes da ata de registro de preços, para que realizem

negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

33.1.2. O fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas, caso não aceite reduzir seu preço aos valores praticados pelo mercado.

Na hipótese prevista na subdivisão acima, o órgão ou entidade gerenciadora convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado, observado o disposto no item 9.1.3.

- O órgão ou entidade gerenciadora cancelará a ata de registro de preços, nos termos do disposto no item 9.2, e adotará as medidas cabíveis para a obtenção de contratação mais vantajosa, caso, nas negociações a que alude a subdivisão acima, os fornecedores do cadastro de reserva não aceitem reduzir seus preços aos valores de mercado.

33.2. Quando o preço praticado no mercado se tornar superior ao preço registrado, o fornecedor poderá requerer ao órgão ou entidade gerenciadora a alteração do preço registrado, desde que observe os requisitos especificados no item 7.2.1.

33.2.1. O requerimento a que alude o item 7.2 deverá observar o disposto no item 6.1 e estar acompanhado de:

a) prova de fato superveniente que impossibilite o cumprimento do compromisso registrado nesta ata;

b) documentação comprobatória da inviabilidade de manutenção do preço registrado.

33.2.2. Na hipótese de não comprovação dos requisitos especificados nos itens 7.2 e 7.2.1:

a) o pedido será indeferido pelo órgão ou entidade gerenciadora;

b) o fornecedor deverá cumprir o compromisso registrado na ata sob pena de cancelamento do seu registro, nos termos do item 9.1, sem prejuízo da aplicação das sanções cabíveis, em especial aquelas previstas na Lei nº 14.133, de 2021.

33.2.3. Quando realizado o cancelamento do registro do fornecedor a que alude a alínea “b” do item 7.2.2, o órgão ou entidade gerenciadora convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no item 5.6.

O órgão ou entidade gerenciadora cancelará a ata de registro de preços, nos termos do item 9.2, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa, caso não obtenha êxito nas negociações a que alude a subdivisão acima.

33.2.4. Quando forem comprovados os requisitos estabelecidos nos itens 7.2 e 7.2.1, o órgão ou entidade gerenciadora:

a) alterará o preço registrado, observados os valores praticados pelo mercado, no limite do impacto causado pelos fatos supervenientes ensejadores da inviabilidade de manutenção do preço inicial;

b) comunicará o novo preço aos órgãos e entidades que tiverem firmado contratos decorrentes desta ata de registro de preços, para eventual alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

34. REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

34.1. As quantidades previstas para os itens com preços registrados nesta ata de registro de preços poderão ser remanejadas pelo órgão ou entidade gerenciadora entre os órgãos ou entidades participantes do registro de preços e, caso seja admitida a adesão no item 4 deste instrumento, órgãos ou entidades não participantes, nas seguintes condições:

a) de órgão ou entidade participante para órgão ou entidade participante; ou

b) de órgão ou entidade participante para órgão ou entidade não participante, caso seja admitida a adesão no item 4 deste instrumento, hipótese em que serão observados os limites previstos no art. 86 da Lei nº 14.133, de 2021.

34.2. O órgão ou entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para fins do remanejamento.

34.3. O órgão ou entidade gerenciadora somente autorizará o remanejamento solicitado que seja justificado pelo solicitante, se houver prévia anuência do fornecedor e do órgão ou entidade que sofrer redução dos quantitativos informados.

35. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

35.1. O órgão ou entidade gerenciadora cancelará o registro do fornecedor quando este:

a) descumprir as condições da ata de registro de preços, sem motivo justificado;

b) se recusar a formalizar a contratação no prazo e condições estabelecidos pela Administração sem justificativa aceitável;

c) não aceitar manter seu preço registrado, na hipótese prevista no item 7.2.2; ou

d) for apenado com sanção prevista no inciso III do *caput* do art. 156 da Lei nº 14.133, de 2021, aplicada no âmbito da Administração Pública do Estado de São Paulo, ou sanção prevista no inciso IV do *caput* do mesmo artigo.

35.1.1. Na hipótese a que alude a alínea “d” da subdivisão anterior, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência desta ata de registro de preços, o órgão ou entidade gerenciadora poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, sendo vedadas novas contratações derivadas desta ata enquanto perdurarem os efeitos da sanção.

35.1.2. O cancelamento de registros nas hipóteses previstas no item 35.1 será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos o contraditório e a ampla defesa.

35.1.3. Quando for cancelado o registro do fornecedor, o órgão ou entidade gerenciadora poderá convocar os fornecedores que compõem o cadastro de reserva, observados a ordem de classificação e o disposto no item 5.6.

35.1.4. O órgão ou entidade participante deverá informar ao órgão ou entidade gerenciadora qualquer das ocorrências previstas no item 9.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

35.2. O órgão ou entidade gerenciadora poderá, justificadamente, cancelar, total ou parcialmente, os preços registrados nesta ata de registro de preços:

a) por razão de interesse público;
b) a pedido do fornecedor, à vista de prova da ocorrência superveniente de caso fortuito ou força maior que impossibilitem o cumprimento do compromisso registrado; ou
c) se não houver êxito nas negociações, nos termos dos itens 7.1.2.1.1 e 7.2.3.1.

36. DAS PENALIDADES

36.1. O descumprimento desta Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no instrumento convocatório mencionado no item 1.1, garantidos o contraditório e a ampla defesa.

36.1.1. As sanções cabíveis também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente.

36.2. É da competência do órgão ou entidade gerenciadora, garantidos o contraditório e a ampla defesa, aplicar as penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço, em relação à sua demanda registrada, ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações.

36.3. É da competência do respectivo órgão ou entidade participante, garantidos o contraditório e a ampla defesa, aplicar as penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preços, em relação à sua demanda registrada, ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações.

36.4. O órgão ou entidade participante deverá informar ao órgão ou entidade gerenciadora as ocorrências de que trata o item 9.1.4, para a finalidade indicada nessa disposição.

37. CONDIÇÕES GERAIS

37.1. Os fornecedores registrados nesta ata de registro de preços estarão obrigados a celebrar as contratações que dela poderão advir nas condições estabelecidas, observado o disposto no instrumento convocatório mencionado no item 1.1 e neste instrumento.

37.1.1. A existência de preços registrados não obriga a Administração a celebrar contratações decorrentes desta ata de registro de preços, observando-se o disposto no item 5.9.

37.2. A contratação com os fornecedores registrados nesta ata será formalizada pelo órgão ou entidade interessada mediante a *assinatura de termo de contrato,* cuja minuta integra como Anexo o instrumento convocatório mencionado no item 1.1.

37.2.1. Se, por ocasião da formalização da contratação, algum dos documentos apresentados pelo fornecedor para fins de comprovação das condições de habilitação estiver com o prazo de validade expirado, o órgão ou entidade interessada verificará a situação por meio eletrônico hábil de informações e certificará a regularidade nos autos do processo, anexando a ele os documentos comprobatórios, salvo impossibilidade devidamente justificada.

37.2.2. Se não for possível atualizar os documentos referidos na subdivisão acima por meio eletrônico hábil de informações, o fornecedor será notificado para, no prazo de *02 (dois) dias úteis*, comprovar a sua situação de regularidade mediante a apresentação das certidões respectivas com prazos de validade em vigência, sob pena de a contratação não se realizar.

37.2.3. Constitui condição para a celebração da contratação, bem como para a realização dos pagamentos dela decorrentes, a inexistência de registros em nome do fornecedor no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais– CADIN ESTADUAL”. Esta condição será considerada cumprida se o devedor comprovar que os respectivos registros se encontram suspensos, nos termos do art. 8º, §§ 1º e 2º, da Lei estadual nº 12.799, de 2008.

37.2.4. Com a finalidade de verificar se o fornecedor mantém as condições de participação no certame, serão novamente consultados, previamente à celebração da contratação, os cadastros especificados no instrumento convocatório mencionado no item 1.1.

37.2.5. Constitui(em), igualmente, condição(ões) para a celebração da contratação:

a apresentação do(s) documento(s) que o fornecedor, à época do certame, houver se comprometido a exibir por ocasião da celebração da contratação por meio de declaração específica, caso exigida na documentação que integra como Anexo o instrumento convocatório mencionado no item 1.1;

a indicação de gestor encarregado de representar o fornecedor com exclusividade perante o Contratante, caso se trate de sociedade cooperativa (se admitida a participação de cooperativa);

caso seja definido no instrumento convocatório mencionado no item 1.1 que o objeto do certame consiste em execução de obra ou serviços de engenharia, a apresentação do registro ou inscrição do fornecedor no Conselho Regional de Engenharia e Agronomia – CREA ou no Conselho de Arquitetura e Urbanismo – CAU competente, com o visto do CREA/SP ou do CAU/SP, conforme o caso, se o local do registro ou inscrição for situado em região não compreendida na área de jurisdição da referida entidade, observada a legislação aplicável.

37.3. O fornecedor terá o prazo de 05 (cinco) dias, contados a partir da data de sua convocação, para assinar o Termo de Contrato, sob pena de decadência, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

37.3.1. O contrato será assinado com a utilização de meio eletrônico, nos termos da legislação aplicável.

37.3.2. O prazo para assinatura previsto na subdivisão anterior poderá ser prorrogado por igual período por solicitação justificada do interessado e aceita pela Administração.

37.3.3. Será considerado celebrado o contrato, em caso de assinaturas por meio eletrônico em datas diferentes, na data da última assinatura eletrônica das partes do termo contratual.

37.4. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos na documentação que integra o instrumento convocatório mencionado no item 1.1.

37.5. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de item(ns) específico(s) do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou entidade.

Para firmeza e validade do pactuado, a presente Ata foi lavrada *em .... (....) via(s)*, que, depois de lida e achada em ordem, vai assinada pelo(a) representante do órgão ou entidade gerenciadora e pelo(as) representante(s) do(s) fornecedor(es) registrado(s), e por testemunhas, todos abaixo identificados*, encaminhando-se cópia ao(s) órgão(s) ou entidade(s) participante(s) mencionado(s) no item 3.2 [se houver].*

Local e data

Assinaturas

Representante legal do órgão ou entidade gerenciadora

Representante(s) legal(is) do(s) fornecedor(s) registrado(s)

TESTEMUNHAS:

1-

2-

Anexo

Cadastro de Reserva

Obedecendo a ordem de classificação, segue relação de fornecedores que aceitaram cotar o(s) item(ns) com preços iguais aos do adjudicatário:

Fornecedor: _____(nome empresarial ou denominação, CNPJ/MF, endereço, contatos, representante)								
Item	*Especificação*	*Marca (se aplicável conforme Edital/ Aviso)*	*Modelo (se aplicável conforme Edital/ Aviso)*	*Unidade*	*Quantidade máxima a ser cotada*	*Quantidade mínima a ser cotada*	*Valor Un*	*Prazo de garantia ou validade (se aplicável conforme Edital/ Aviso)*

Obedecendo a ordem de classificação, segue relação de fornecedores que mantiveram sua proposta original:

Fornecedor: _____(nome empresarial ou denominação, CNPJ/MF, endereço, contatos, representante)								
Item	*Especificação*	*Marca (se aplicável conforme Edital/ Aviso)*	*Modelo (se aplicável conforme Edital/ Aviso)*	*Unidade*	*Quantidade máxima a ser cotada*	*Quantidade mínima a ser cotada*	*Valor Un*	*Prazo de garantia ou validade (se aplicável conforme Edital/ Aviso)*