Parecer 230/2022 – PROJU
Processo: 6600/2022 – SEMAD

CONTRATAÇÃO DE EMPRESA VENCEDORA DE REGISTRO DE PREÇOS. ADESÃO A ATA DE REGISTRO DE PREÇOS. FIGURA DO "CARONA". POSSIBILIDADE.

I – RELATÓRIO

1. Trata-se de consulta formulada pela **SEMAD**, acerca da contratação da empresa **QUALITEK TECNOLOGIA LTDA** através de **Adesão a Ata de Registro de Preços nº 93/2021, realizada por meio de PREGÃO ELETRÔNICO SRP Nº 39/2021**, cujo órgão gerenciador é o **TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS.**

2. Pretende-se através da adesão mencionada adquirir licenças de antivírus para segurança digital dos equipamentos da Prefeitura Municipal de Alagoinhas, entendendo que a solução apresentada se mostra vantajosa para o interesse público.

3. A Secretaria informa que realizou pesquisa de preço e identificou que os valores obtidos no mencionado pregão SRP nº 39/2021 do TJ-TO estavam vantajosos de modo que enviaram ofício ao órgão consultando acerca da possibilidade de adesão, pelo que foi positivamente respondida. Assim, os autos foram instruídos com a justificativa da SEMAD, pesquisa de preços, peças da licitação, consulta ao TJ-TO e a respectiva autorização.

   Segue parecer.

II - FUNDAMENTAÇÃO

4. Ao cuidar das compras, definiu a Lei 8666/1993– artigo 15, inciso II – *que essas deverão ser, sempre que possível, processadas através de sistema de registro de preços.* Tal sistema também foi previsto no artigo 11 da Lei Federal n.º 10.520, de 17 de julho de 2002, que instituiu o Pregão para aquisição de bens e serviços comuns.

5. Com o escopo de regulamentar o sistema de registro de preços, foi expedido, no âmbito federal, o Decreto n.º 3.931, de 19 de setembro de 2001, hoje em vigor com as alterações introduzidas pelo Decreto n.º 4.342, de 23 de agosto de 2002. Tal Decreto, entre as inovações trazidas, instituiu em seu artigo 8º a possibilidade de adesão à ata de registro de preços por outros órgãos e entidades da Administração Pública que não tenham participado da licitação. **É a chamada figura do carona.**

6. Entre as inovações trazidas pelo Decreto n.º 3.931/01, destaca-se a constante do artigo 8º, *verbis:*

> *Art. 8º A Ata de Registro de Preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração que não tenha participado do certame licitatório, mediante prévia consulta ao órgão gerenciador, desde que devidamente comprovada a vantagem.*
> *§ 1º Os órgãos e entidades que não participaram do registro de preços, quando desejarem fazer uso da Ata de Registro de Preços, deverão manifestar seu interesse junto ao órgão gerenciador da Ata, para que este indique os possíveis fornecedores e respectivos preços a serem praticados, obedecida a ordem de classificação.*
> *§ 2º Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento independentemente dos quantitativos registrados em Ata, desde que este fornecimento não prejudique as obrigações anteriormente assumidas.*
> *§ 3 As aquisições ou contratações adicionais a que se refere este artigo não poderão exceder, por órgão ou entidade, a cem por cento dos quantitativos registrados na Ata de Registro de Preços. (Incluído pelo Decreto nº 4.342, de 23.8.2002)*

7. **JORGE ULISSES JACOBY FERNANDES** conceitua o sistema de registro de preços da seguinte forma:

> *É um procedimento especial de licitação que se efetiva por meio de uma concorrência ou pregão sui generis, selecionando a proposta mais vantajosa, com observância do princípio da isonomia, para eventual e futura contratação pela Administração.* (FERNANDES, Jorge Ulisses Jacoby. Carona em sistema de registro de preços: uma opção inteligente para redução de custos e controle. 2007. p. 31)

8. Mencionado doutrinador, analisando o art. 8º do Decreto nº 3931/01, relaciona para a adesão à Ata de Registro de Preços os seguintes requisitos:

> a) Interesse do órgão não participante (carona) em utilizar a Ata de Registro de Preços;
> b) Avaliação em processo próprio, interno do órgão não participante (carona) de que os preços e condições do SRP são mais vantajosos, fato que pode ser revelado em simples pesquisa;
> c) Prévia consulta e anuência do órgão gerenciador;
> d) Indicação pelo órgão gerenciador do fornecedor, com observância da ordem de classificação;
> e) Aceitação, pelo fornecedor, da contratação pretendida, condicionada à ausência de prejuízo aos compromissos assumidos na Ata de Registro de Preços;
> f) Embora a norma seja silente a respeito, deverão ser mantidas as mesmas condições do registro, ressalvadas apenas as renegociações promovidas pelo órgão gerenciador, que se fizerem necessárias;
> g) Limitação da quantidade a cem por cento dos quantitativos registrados na Ata.

9. Assim, nota-se que a vantagem econômica deve estar devidamente comprovada, o que deve ser feito por meio de ampla pesquisa de preços praticados no mercado local e no âmbito da Administração Pública de bens ou serviços com especificações compatíveis com aqueles que se pretende contratar.

10. Nesse aspecto, registra-se que o Sistema de Registro de Preços, como procedimento especial de licitação, deve ser regido pelos princípios relacionados na Lei n.º 8.666/1993. Referido diploma legal, em seu art. 3º, preceitua que *"a licitação destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração e será processada e julgada em estrita conformidade com o princípio da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos".*

11. Nesse sistema a Administração Pública indica – como em qualquer licitação – o objeto que pretende adquirir e informa os quantitativos estimados e máximos pretendidos. Diferentemente, porém, da licitação convencional, não assume o compromisso de contratação, nem mesmo de quantitativos mínimos. A consumação da contratação somente ocorre se houver necessidade. O licitante compromete-se a manter durante o prazo definido a disponibilidade do produto nos quantitativos máximos pretendidos.

12. Desse modo, o Sistema de Registro de Preços constitui em importante instrumento de gestão onde as demandas são incertas, frequentes ou de difícil mensuração. Por outro lado, como já decidiu o **TRIBUNAL DE CONTAS DA UNIÃO** também pode ser utilizado para objetos que dependem de outras variáveis inibidoras do uso da licitação convencional, tal como ocorre com um Município que aguarda recursos de convênios – muitas vezes transferidos em final de exercício com prazo restrito para a aplicação; liberados os recursos se o objeto já houver sido licitado pelo Sistema de Registro de Preços caberá apenas expedir a nota de empenho para consumar a contratação.

> Nesse sentido: *Sistema de Registro de Preços – deve ser regra sempre que presente uma das hipóteses permissivas, processar, preferencialmente, as aquisições de bens por intermédio do Sistema de Registro de Preços.* (Fonte: TCU – Plenário - Prestação de Contas. Acórdão 56/1999).

13. No caso em tela, a SEMAD, diante da necessidade de aquisição de licenças para programas antivírus

destinados a proteção da infraestrutura de rede e dos computadores da prefeitura, realizou estudos preliminares e pesquisa de mercado, verificando a existência da ata em questão, oriunda de pregão eletrônico realizado pelo Tribunal de Justiça do Tocantins que possuía preços mais vantajosos do que aqueles obtidos na pesquisa.

14. Verifico que foi realizada a consulta ao órgão gestor da ata e obtida a autorização como consta nos autos, de modo que a empresa foi também contatada e concordou em fornecer, enviando a documentação anexa.

15. Nesse sentido, cumpre esclarecer que a conveniência e oportunidade da medida em questão é competência da Secretaria solicitante, que deverá observar os requisitos aqui apontados, validando a autenticidade dos documentos acostados e atestando a efetiva vantajosidade da medida ao interesse público.

III – CONCLUSÃO

16. Isto posto, com base nas argumentações expostas e doutrina citada e com fundamento legal no **art. 15 e seguintes da lei 8666/93 e art. 8º do Decreto Federal nº 3931/2001,** opinamos pela possibilidade da **Adesão a Ata de Registro de Preços nº 93/2021,** realizada por meio de **PREGÃO ELETRÔNICO RP Nº 39/2021**, cujo órgão gerenciador é o **TJ-TO.**

É o parecer. Salvo melhor juízo.

Alagoinhas/BA, 02 de junho de 2022.

WALTER FREITAS MEDEIROS NETO
Procurador Administrativo

ESTADO DA BAHIA
PREFEITURA MUNICIPAL DE ALAGOINHAS
COMISSÃO TÉCNICA DE AVALIAÇÃO ORÇAMENTÁRIA E FINANCEIRA

DADOS DO PROCESSO

Processo n.º: 06600/2022 Data: 30 / 05 / 2022

Unidade Requisitante: SEMAD

Objeto: ADESÃO À ATA 93/2021-TJTO, REFERENTE AO PREGÃO 39/2021 PARA CONTRATAÇÃO DE EMPRESA PARA AQUISIÇÃO DE LICENÇA DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS KASPERSKY ENDROPOINT-VERSÃO BUSINESS SELECT, INCLUINDO ATUALIZAÇÕES E SUPORTE TÉCNICO.

DADOS ANALISADOS	APROVADO	REPROVADO	PARECER
Valor do Processo			

DELIBERAÇÕES

→ SD SEM ASSINATURA DO SECRETÁRIO, OK!
→ AUSÊNCIA NO PROCESSO DAS PESQUISAS DE PREÇOS COMPARATIVOS CITADAS NA JUSTIFICATIVA, OK!.

ASSINATURAS COMISSÃO TÉCNICA

Karin - SEPLA	Juliana- SEFAZ	Jeorrice -COGER	Mariane -SEMAD	Ana Verena- PROJU

Prefeitura Municipal de Alagoinhas
Fone/Fax: 7534238306/
E-mail:
Graciliano de Freitas, s/n -
CEP: 48010100
CNPJ: 13.646.005/0001-38

Protocolo de Processo

6600/2022

Interessado(s)

Número do CGM:	5081
Nome:	Secretaria Municipal de Administracao
Endereço:	Manoel Romao, 0
Bairro:	Alagoinhas Velha
Cep:	48010100
Cidade:	Alagoinhas
CNPJ/CPF:	

Dados do Processo

Data de Entrada:	27/05/2022 10:11
Situação do Processo:	Em andamento, a receber
Classificação:	Requisicao
Assunto:	Contrato
Setor Inicial:	01.04.05.00 - Diretoria de Tecnologia da Informação SEMAD
Destino:	01.17.02.00 - Proju Copel
Observações:	Adesão a ATA 93/2021 - TJTO, referente ao Pregão 39/2021 para Contratação de empresa para aquisição de licença de solução corporativa de antivírus Karspersky Endropoint - versão Business Select, incluindo atualizações e suporte técnico.

Atributos de Assunto de Processo

Documentação

Requisicao Recebido

Requerimento

Prefeitura Municipal de Alagoinhas, 30 de Maio de 2022.

Mariane A. C. Martins
Agente de Planejamento

PREFEITURA MUNICIPAL DE ALAGOINHAS
CONTROLADORIA GERAL DO MUNICÍPIO
NÚCLEO DE CONTROLE

PARECER/COGER
Nº 160/2022

PROCESSO: n° 6600/2022
SECRETARIA SOLICITANTE: SEMAD
PARECER JURÍDICO: n°230/2022
CONTRATO: n° 248/2022
ADESÃO A ATA DE REGISTRO DE PREÇO: n° 93/2021 – REALIZADA POR MEIO DE PREGÃO ELETRÔNICO – SRP N° 39/2021
ORGÃO GERENCIADOR: TRIBUNAL DE JUSTIÇA DO ESTADO DE TOCANTINS

Em face da autorização do Processo de número em epígrafe, vieram os autos encaminhados pelo **NÚCLEO DE CONTRATOS** ao Gabinete desta Controladoria para análise e elaboração do Parecer Técnico.

O referido processo tem por objeto **AQUISIÇÃO DE LICENÇA DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS KASPERSKY ENDPOINT SECURITY – VERSÃO BUSINESS SELECT, INCLUINDO ATUALIZAÇÕES E SUPORTE TÉCNICO,** e analisando os dados inseridos no processo, Justificativa de adesão e Justificativa técnica, Oficio de autorização do TJ-TO de adesão à Ata, Oficio de aceite da empresa a adesão a Ata, Peças da licitação, Pesquisa de preço, Pedido de Realização de Despesas-PRDC, Parecer Jurídico de nº 230/2022, e demais documentos, vislumbra-se que o referido processo apresenta as condições determinadas pelas Leis 8.666/93 e suas alterações posteriores.

A Controladoria após analisar o aspecto formal recomenda o prosseguimento da Adesão a **ATA DE REGISTRO DE PREÇO** em favor da empresa **QUALITEK TECNOLOGIA – LTDA.**

É o Parecer.

Alagoinhas, 30 de junho de 2022.

Deisianny dos S. Andrade
Coordenadora

Leila Carla Vila Flor Souza Gabriel
Controladora Geral do Município

PREFEITURA MUNICIPAL DE ALAGOINHAS
CONTROLADORIA GERAL DO MUNICÍPIO
NÚCLEO DE CONTROLE

DESPACHO/COGER
Nº 160/2022

PROCESSO: n° 6600/2022
SECRETARIA SOLICITANTE: SEMAD
PARECER JURÍDICO: n°230/2022
CONTRATO: n° 248/2022
ADESÃO A ATA DE REGISTRO DE PREÇO: n° 93/2021 – REALIZADA POR MEIO DE PREGÃO ELETRÔNICO – SRP N° 39/2021
ORGÃO GERENCIADOR: TRIBUNAL DE JUSTIÇA DO ESTADO DE TOCANTINS

Em face da autorização do Processo de número em epígrafe, vieram os autos encaminhados pelo **NÚCLEO DE CONTRATOS** ao Gabinete desta Controladoria para análise e elaboração do Parecer Técnico.

O referido processo tem por objeto a **AQUISIÇÃO DE LICENÇA DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS KASPERSKY ENDPOINT SECURITY – VERSÃO BUSINESS SELECT, INCLUINDO ATUALIZAÇÕES E SUPORTE TÉCNICO** e, analisando os documentos juntados ao supracitado processo, este Controle Interno relaciona abaixo o seguinte apontamento:

- Adequar objeto do contrato conforme objeto contratado pelo município; OK
- Adequar no contrato informações do estado para a do município;
- Conforme informação n° 17106/2022 não foi localizado no processo o item 4 e 6 recomendado, porém não é impedimento para prosseguimento do processo.

É o Despacho.

Alagoinhas, 21 de junho de 2022.

Deisianny dos S. Andrade
Coordenadora

Leila Carla Vila Flor Souza Gabriel
Controladora Geral do Município

PREFEITURA MUNICIPAL DE ALAGOINHAS
CONTROLADORIA GERAL DO MUNICÍPIO
NÚCLEO DE CONTROLE

DESPACHO/COGER
Nº 160/2022

PROCESSO: n° 6600/2022
SECRETARIA SOLICITANTE: SEMAD
PARECER JURÍDICO: n°230/2022
CONTRATO: n° 248/2022
ADESÃO A ATA DE REGISTRO DE PREÇO: n° 93/2021 – REALIZADA POR MEIO DE PREGÃO ELETRÔNICO – SRP N° 39/2021
ORGÃO GERENCIADOR: TRIBUNAL DE JUSTIÇA DO ESTADO DE TOCANTINS

Em face da autorização do Processo de número em epígrafe, vieram os autos encaminhados pelo **NÚCLEO DE CONTRATOS** ao Gabinete desta Controladoria para análise e elaboração do Parecer Técnico.

O referido processo tem por objeto a **AQUISIÇÃO DE LICENÇA DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS KASPERSKY ENDPOINT SECURITY – VERSÃO BUSINESS SELECT, INCLUINDO ATUALIZAÇÕES E SUPORTE TÉCNICO** e, analisando os documentos juntados ao supracitado processo, este Controle Interno relaciona abaixo o seguinte apontamento:

- Adequar objeto do contrato conforme objeto contratado pelo município;
- Adequar no contrato informações do estado para a do município;
- Conforme informação n° 17106/2022 não foi localizado no processo o item 4 e 6 recomendado, porém não é impedimento para prosseguimento do processo.

É o Despacho.

Alagoinhas, 21 de junho de 2022.

Deisianny dos S. Andrade
Coordenadora

Leila Carla Vila Flor Souza Gabriel
Controladora Geral do Município

Histórico do Empregador

O Histórico do Empregador apresenta os registros dos CRF concedidos nos últimos 24 meses, conforme Manual de Orientações Regularidade do Empregador.

Inscrição: 10.224.281/0001-10
Razão social: QUALITEK TECNOLOGIA LTDA
Nome fantasia: QUALITEK

Data de Emissão/Leitura	Data de Validade	Número do CRF
12/07/2022	12/07/2022 a 10/08/2022	2022071201333558928862
23/06/2022	23/06/2022 a 22/07/2022	202206230l373081552673
04/06/2022	04/06/2022 a 03/07/2022	202206040l352048450048
16/05/2022	16/05/2022 a 14/06/2022	202205160305204598660 5
27/04/2022	27/04/2022 a 26/05/2022	20220427012023078874 55
08/04/2022	08/04/2022 a 07/05/2022	202204080l320188431197
20/03/2022	20/03/2022 a 18/04/2022	20220320010204995837 25
01/03/2022	01/03/2022 a 30/03/2022	2022030101190597602401
10/02/2022	10/02/2022 a 11/03/2022	202202100l240507550692
22/01/2022	22/01/2022 a 20/02/2022	20220122051010709913 60
30/12/2021	30/12/2021 a 28/01/2022	2021123001314901521101
11/12/2021	11/12/2021 a 09/01/2022	202112110l285926941814
22/11/2021	22/11/2021 a 21/12/2021	20211122011026102917 50
03/11/2021	03/11/2021 a 02/12/2021	2021110301171404893660
15/10/2021	15/10/2021 a 13/11/2021	2021101501363563038102
26/09/2021	26/09/2021 a 25/10/2021	202109260l144216593855
07/09/2021	07/09/2021 a 06/10/2021	202109070l474666883020
19/08/2021	19/08/2021 a 17/09/2021	202108190l400102973890
31/07/2021	31/07/2021 a 29/08/2021	202107310l324482175228
13/04/2021	13/04/2021 a 10/08/2021	202104130l444293218130
25/03/2021	25/03/2021 a 23/04/2021	202103250l283813093618
06/03/2021	06/03/2021 a 04/04/2021	202103060l201168045217
15/02/2021	15/02/2021 a 16/03/2021	202102150l303294433417
27/01/2021	27/01/2021 a 25/02/2021	202101270303070512813603
08/01/2021	08/01/2021 a 06/02/2021	202101080318540586921 7
20/12/2020	20/12/2020 a 18/01/2021	20201220143015341305 37
01/12/2020	01/12/2020 a 30/12/2020	202012010302338435410 9
12/11/2020	12/11/2020 a 11/12/2020	202011120225286214416 5
24/10/2020	24/10/2020 a 22/11/2020	20201024022449424494 40
05/10/2020	05/10/2020 a 03/11/2020	20201005044301540383 07

Voltar | Imprimir

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 10.224.281/0001-10
Razão Social: QUALITEK TECNOLOGIA LTDA
Endereço: R JOSE RIBEIRO DANTAS 275 SALA 404 SALA 406 / LAGOA NOVA / NATAL / RN / 59062-480

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade: 12/07/2022 a 10/08/2022

Certificação Número: 2022071201333558928862

Informação obtida em 13/07/2022 10:10:52

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

CERTIDÃO ESTADUAL

Falência e/ou Recuperação Judicial e Extrajudicial

CERTIDÃO Nº: 9998818/2022 **FOLHA 2/2**

Esta certidão terá validade de 30 dias corridos, contados a partir da data de expedição do documento.

Código autenticador: 5a3b07793d98276be8419011f720b02c

A autenticidade dessas informações pode ser verificada por meio do endereço eletrônico: https://apps.tjrn.jus.br/certidoes/f/public/index.xhtml

Estado do Rio Grande do Norte, Quarta-feira, 29 de Junho de 2022 às 09:03

PODER JUDICIÁRIO

ESTADO DO RIO GRANDE DO NORTE

Data Emissão
29/06/2022

CERTIDÃO ESTADUAL

Falência e/ou Recuperação Judicial e Extrajudicial

CERTIDÃO Nº: 9998818/2022 **FOLHA 1/2**

Certifico que, pesquisando os registros de distribuições de feitos do Estado do Rio Grande do Norte, no período de 20 anos, verifiquei NADA CONSTAR em nome de:

Nome: QUALITEK TECNOLOGIA LTDA

CPF/CNPJ: 10.224.281/0001-10

RG:

Endereço: Rua José Ribeiro Dantas, 275, Lagoa Nova, Natal/RN, 59062-480

Data Nascimento:

Nome Mãe:

Nome Pai:

Na hipótese de haver processos com Segredo de Justiça e Sigilo Externo, não serão informados nessa Certidão.

CERTIFICO, outrossim, que os dados pessoais, constantes nesta certidão, foram informados pelo solicitante, devendo sua titularidade ser conferida pelo interessado e destinatário.

Esta certidão abrange a 1ª Instância da Justiça Estadual do RN.

O TJRN CERTIFICA AINDA, que a pesquisa dos registros de distribuições de feitos cíveis, envolvendo as Ações de Falência e Recuperação Judicial e Extrajudicial, inclui também os procedimentos do Decreto Lei n. 7.661, de 21 de junho de 1945.

CERTIFICA finalmente, que esta certidão, pode ter sua autenticidade confirmada no endereço eletrônico www.tjrn.jus.br, no campo Consultas / Emissão e autenticação de certidão, informando-se o seu número, por um prazo máximo de 30 (trinta) dias de validade.

Esta certidão está sendo emitida com base na busca processual realizada na base de dados unificada do GPS-JUS, em 29/06/2022 09:03. Esta é uma base consolidada do TJRN que contempla os seguintes sistemas: PJE (1º e 2º Grau), SAJ (1º e 2º Grau) e SEEU.

GOVERNO DO ESTADO DO RIO GRANDE DO NORTE
Secretaria de Estado da Tributação
Procuradoria Geral do Estado

CERTIDÃO CONJUNTA NEGATIVA Nº 7374353
DE DÉBITOS RELATIVOS AOS TRIBUTOS ESTADUAIS E À DÍVIDA ATIVA DO ESTADO

Contribuinte: **QUALITEK TECNOLOGIA LTDA**
CNPJ: **10.224.281/0001-10** Inscrição Estadual: **20.243.835-0**

Certificamos que, até a presente data, não constam pendências em nome do sujeito passivo acima especificado, referente a tributos estaduais ou débitos inscritos na Dívida Ativa Estadual, ressalvada à Fazenda Pública o direito de cobrar quaisquer dívidas que venham a ser apuradas.

Esta certidão refere-se exclusivamente à situação do sujeito passivo no âmbito da Secretaria de Estado de Tributação e da Procuradoria Geral do Estado, não abrangendo as taxas e contribuições devidas aos demais órgãos do Estado, exceto se inscritas na Dívida Ativa.

ASPECTOS DE VALIDADE

A autenticidade desta certidão deverá ser verificada na Internet, no endereço https://uvt2.set.rn.gov.br/#/services/autenticidade/certidao-conjunta.

Certidão emitida com base no Decreto Estadual nº 30.416, de 15/03/2021.

Emitida em **25/05/2022** às **09:38:50** <Horário de Natal/RN>.

Endereço IP: **179.190.240.132.**

Validade até **21/09/2022**.

Certidão emitida gratuitamente.

Atenção: Qualquer rasura ou emenda invalidará este documento.

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

Nome: QUALITEK TECNOLOGIA LTDA (MATRIZ E FILIAIS)
CNPJ: 10.224.281/0001-10
Certidão nº: 16783522/2022
Expedição: 26/05/2022, às 15:31:12
Validade: 22/11/2022 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que **QUALITEK TECNOLOGIA LTDA (MATRIZ E FILIAIS)**, inscrito(a) no CNPJ sob o nº **10.224.281/0001-10, NÃO CONSTA** como inadimplente no Banco Nacional de Devedores Trabalhistas.
Certidão emitida com base nos arts. 642-A e 883-A da Consolidação das Leis do Trabalho, acrescentados pelas Leis ns.º 12.440/2011 e 13.467/2017, e no Ato 01/2022 da CGJT, de 21 de janeiro de 2022.
Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho.
No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.
A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (http://www.tst.jus.br).
Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE
Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho, Comissão de Conciliação Prévia ou demais títulos que, por disposição legal, contiver força executiva.

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: QUALITEK TECNOLOGIA LTDA
CNPJ: 10.224.281/0001-10

Ressalvado o direito de a Fazenda Nacional cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado que vierem a ser apuradas, é certificado que não constam pendências em seu nome, relativas a créditos tributários administrados pela Secretaria da Receita Federal do Brasil (RFB) e a inscrições em Dívida Ativa da União (DAU) junto à Procuradoria-Geral da Fazenda Nacional (PGFN).

Esta certidão é válida para o estabelecimento matriz e suas filiais e, no caso de ente federativo, para todos os órgãos e fundos públicos da administração direta a ele vinculados. Refere-se à situação do sujeito passivo no âmbito da RFB e da PGFN e abrange inclusive as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991.

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, nos endereços <http://rfb.gov.br> ou <http://www.pgfn.gov.br>.

Certidão emitida gratuitamente com base na Portaria Conjunta RFB/PGFN nº 1.751, de 2/10/2014.
Emitida às 14:27:13 do dia 23/02/2022 <hora e data de Brasília>.
Válida até 22/08/2022.
Código de controle da certidão: **8039.9343.73A6.3DB3**
Qualquer rasura ou emenda invalidará este documento.

Prefeitura Municipal do Natal

SEMUT - Secretaria Municipal de Tributação

Certidão Negativa de Débitos para com a Fazenda Municipal

Nº da Certidão:	Código de Validação:	Observação:
2359096	338824480693	A validade desta certidão deve ser verificada utilizando o código ao lado, pela internet, no endereço www.natal.rn.gov.br/semut

Contribuinte:

CPF/CNPJ:	Nome/Razão Social:
10.224.281/0001-10	QUALITEK TECNOLOGIA LTDA - EPP
Situação Cadastral:	EMPRESA COM INSCRIÇÃO MOBILIÁRIA ATIVA NO MUNICÍPIO

Inscrições Mobiliárias Ativas:
167.926-0 - 10.224.281/0001-10

Certificamos que, até a presente data, não consta em nossos arquivos crédito de natureza tributária vencido, irregularidades cadastrais, irregularidades na apresentação de Declarações e crédito de natureza não tributária inscrito em dívida ativa, de responsabilidade do contribuinte acima qualificado, ficando ressalvado à Fazenda Municipal o direito de cobrar qualquer dívida que venha a ser apurada.

A presente Certidão foi expedida com base no artigo 4º da Lei Complementar nº 168 de 13/09/2017 combinado com a Portaria nº 004/2018-GS/SEMUT.

Validade:
Esta certidão é válida por 30 dias a contar da data de sua expedição

Local e Data de Expedição:
Natal (RN), 29 de junho de 2022

Emitida pela sessão: 408650815 através do IP: 179.190.240.132

PODER JUDICIÁRIO

ESTADO DO RIO GRANDE DO NORTE

Data Emissão
19/07/2022

CERTIDÃO ESTADUAL

Falência e/ou Recuperação Judicial e Extrajudicial

CERTIDÃO Nº: 5942356/2022 **FOLHA 1/2**

Certifico que, pesquisando os registros de distribuições de feitos do Estado do Rio Grande do Norte, no período de 20 anos, verifiquei NADA CONSTAR em nome de:

Nome: QUALITEK TECNOLOGIA LTDA

CPF/CNPJ: 10.224.281/0001-10

RG:

Endereço: Rua José Ribeiro Dantas,275 sala 406, Lagoa Nova, Natal/RN, 59062-480

Data Nascimento:

Nome Mãe:

Nome Pai:

Na hipótese de haver processos com Segredo de Justiça e Sigilo Externo, não serão informados nessa Certidão.

CERTIFICO, outrossim, que os dados pessoais, constantes nesta certidão, foram informados pelo solicitante, devendo sua titularidade ser conferida pelo interessado e destinatário.

Esta certidão abrange a 1ª Instância da Justiça Estadual do RN.

O TJRN CERTIFICA AINDA, que a pesquisa dos registros de distribuições de feitos cíveis, envolvendo as Ações de Falência e Recuperação Judicial e Extrajudicial, inclui também os procedimentos do Decreto Lei n. 7.661, de 21 de junho de 1945.

CERTIFICA finalmente, que esta certidão, pode ter sua autenticidade confirmada no endereço eletrônico www.tjrn.jus.br, no campo Consultas / Emissão e autenticação de certidão, informando-se o seu número, por um prazo máximo de 30 (trinta) dias de validade.

Esta certidão está sendo emitida com base na busca processual realizada na base de dados unificada do GPS-JUS, em 19/07/2022 09:22. Esta é uma base consolidada do TJRN que contempla os seguintes sistemas: PJE (1º e 2º Grau), SAJ (1º e 2º Grau) e SEEU.

CERTIDÃO ESTADUAL

Falência e/ou Recuperação Judicial e Extrajudicial

CERTIDÃO Nº: 5942356/2022

Esta certidão terá validade de 30 dias corridos, contados a partir da data de expedição do documento.

Código autenticador: 749ce6c3d833e25cf801de27fabe8aac

A autenticidade dessas informações pode ser verificada por meio do endereço eletrônico: https://apps.tjrn.jus.br/certidoes/f/public/index.xhtml

Estado do Rio Grande do Norte, Terça-feira, 19 de Julho de 2022 às 09:22

GOVERNO DO ESTADO DO RIO GRANDE DO NORTE
Secretaria de Estado da Tributação
Procuradoria Geral do Estado

CERTIDÃO CONJUNTA NEGATIVA Nº 7374353
DE DÉBITOS RELATIVOS AOS TRIBUTOS ESTADUAIS E À DÍVIDA ATIVA DO ESTADO

Contribuinte: **QUALITEK TECNOLOGIA LTDA**
CNPJ: **10.224.281/0001-10** Inscrição Estadual: **20.243.835-0**

Certificamos que, até a presente data, não constam pendências em nome do sujeito passivo acima especificado, referente a tributos estaduais ou débitos inscritos na Dívida Ativa Estadual, ressalvada à Fazenda Pública o direito de cobrar quaisquer dívidas que venham a ser apuradas.

Esta certidão refere-se exclusivamente à situação do sujeito passivo no âmbito da Secretaria de Estado de Tributação e da Procuradoria Geral do Estado, não abrangendo as taxas e contribuições devidas aos demais órgãos do Estado, exceto se inscritas na Dívida Ativa.

ASPECTOS DE VALIDADE

A autenticidade desta certidão deverá ser verificada na Internet, no endereço https://uvt2.set.rn.gov.br/#/services/autenticidade/certidao-conjunta.

Certidão emitida com base no Decreto Estadual nº 30.416, de 15/03/2021.

Emitida em **25/05/2022** às **09:38:50** <Horário de Natal/RN>.

Endereço IP: **179.190.240.132**.

Validade até **21/09/2022**.

Certidão emitida gratuitamente.

Atenção: Qualquer rasura ou emenda invalidará este documento.

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

Nome: QUALITEK TECNOLOGIA LTDA (MATRIZ E FILIAIS)
CNPJ: 10.224.281/0001-10
Certidão nº: 16783522/2022
Expedição: 26/05/2022, às 15:31:12
Validade: 22/11/2022 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que **QUALITEK TECNOLOGIA LTDA (MATRIZ E FILIAIS)**, inscrito(a) no CNPJ sob o nº **10.224.281/0001-10, NÃO CONSTA** como inadimplente no Banco Nacional de Devedores Trabalhistas.
Certidão emitida com base nos arts. 642-A e 883-A da Consolidação das Leis do Trabalho, acrescentados pelas Leis ns.º 12.440/2011 e 13.467/2017, e no Ato 01/2022 da CGJT, de 21 de janeiro de 2022.
Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho.
No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.
A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (http://www.tst.jus.br).
Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE
Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho, Comissão de Conciliação Prévia ou demais títulos que, por disposição legal, contiver força executiva.

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: QUALITEK TECNOLOGIA LTDA
CNPJ: 10.224.281/0001-10

Ressalvado o direito de a Fazenda Nacional cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado que vierem a ser apuradas, é certificado que não constam pendências em seu nome, relativas a créditos tributários administrados pela Secretaria da Receita Federal do Brasil (RFB) e a inscrições em Dívida Ativa da União (DAU) junto à Procuradoria-Geral da Fazenda Nacional (PGFN).

Esta certidão é válida para o estabelecimento matriz e suas filiais e, no caso de ente federativo, para todos os órgãos e fundos públicos da administração direta a ele vinculados. Refere-se à situação do sujeito passivo no âmbito da RFB e da PGFN e abrange inclusive as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991.

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, nos endereços <http://rfb.gov.br> ou <http://www.pgfn.gov.br>.

Certidão emitida gratuitamente com base na Portaria Conjunta RFB/PGFN nº 1.751, de 2/10/2014.
Emitida às 14:27:13 do dia 23/02/2022 <hora e data de Brasília>.
Válida até 22/08/2022.
Código de controle da certidão: **8039.9343.73A6.3DB3**
Qualquer rasura ou emenda invalidará este documento.

Prefeitura Municipal do Natal

SEMUT - Secretaria Municipal de Tributação

Certidão Negativa de Débitos para com a Fazenda Municipal

Nº da Certidão:	Código de Validação:	Observação:
2373609	156858916478	A validade desta certidão deve ser verificada utilizando o código ao lado, pela internet, no endereço www.natal.rn.gov.br/semut

Contribuinte:

CPF/CNPJ:	Nome/Razão Social:
10.224.281/0001-10	QUALITEK TECNOLOGIA LTDA - EPP
Situação Cadastral:	EMPRESA COM INSCRIÇÃO MOBILIÁRIA ATIVA NO MUNICÍPIO

Inscrições Mobiliárias Ativas:
167.926-0 - 10.224.281/0001-10

Certificamos que, até a presente data, não consta em nossos arquivos crédito de natureza tributária vencido, irregularidades cadastrais, irregularidades na apresentação de Declarações e crédito de natureza não tributária inscrito em dívida ativa, de responsabilidade do contribuinte acima qualificado, ficando ressalvado à Fazenda Municipal o direito de cobrar qualquer dívida que venha a ser apurada.

A presente Certidão foi expedida com base no artigo 4º da Lei Complementar nº 168 de 13/09/2017 combinado com a Portaria nº 004/2018-GS/SEMUT.

Validade:
Esta certidão é válida por 30 dias a contar da data de sua expedição

Local e Data de Expedição:
Natal (RN), 19 de julho de 2022

Emitida pela sessão: 410550862 através do IP: 177.37.203.83

Voltar | Imprimir

CAIXA
CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 10.224.281/0001-10
Razão Social: QUALITEK TECNOLOGIA LTDA
Endereço: R JOSE RIBEIRO DANTAS 275 SALA 404 SALA 406 / LAGOA NOVA / NATAL / RN / 59062-480

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade: 12/07/2022 a 10/08/2022

Certificação Número: 2022071201333558928862

Informação obtida em 13/07/2022 10:10:52

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

ESTADO DA BAHIA
PREFEITURA MUNICIPAL DE ALAGOINHAS
Pça. Graciliano de Freitas. S/N, Centro
CNPJ: 13.646.005/0001-38

PEDIDO DE REALIZAÇÃO DE DESPESA E CONTRATAÇÃO

1.Nº	2.UNIDADE REQUISITANTE (SIGLA)	3.DATA DE EMISSÃO: (DD/MM/AAAA)	4.ÓRGÃO DESTINO (SIGLA):
072/2022	SEMAD	27/05/2022	SEPLA

5.NECESSIDADE	6.JUSTIFICATIVA	7.VIGÊNCIA
Adesão a ata 93/2021 - TJTO, referente ao pregão eletrônico nº 39/2021 para contratação de empresa para a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – versão business select, incluindo atualizações e suporte técnico.	A Solução se caracteriza por garantir a segurança de computadores desktop, servidores e notebooks, assim como a proteção dos serviços e sistemas providos por esta administração. Partimos da premissa de que o ambiente computacional da Prefeitura Municipal de Alagoinhas e suas diversas secretarias devem estar tecnologicamente atualizado, a fim de atender as demandas relativas à necessidade de segurança cibernética. Diante disso, solicitamos a Adesão da Ata de Registro de Preços nº 39/2021 do Tribunal de Justiça do Estado do Tocantins.	36 meses

8.INFORMAÇÕES ORÇAMENTÁRIA / FINANCEIRA

Projeto/Atividade	Elemento de Despesa	Fonte de Recurso	Disponibilidade Financeira
2196 – SEMAD	3.3.90.40	500.0000	

9.FORMA DE PAGAMENTO:	10.PRAZO/LOCAL DA ENTREGA:
1 (uma) única parcela.	Diretoria de Tecnologia da Informação - SEMAD

11.ITEM	12.CÓD	13.DISCRIMINAÇÃO DO PEDIDO	14.UNID	15.QTD	16.VALORES	
					UNIT.	TOTAL
1		Contratação de empresa para aquisição de licença de uso de software antivírus de rede, incluindo instalação e suporte.				R$ 27.750,00
17.VALOR TOTAL ESTIMADO ==========>						R$ 27.750,00

18.SECRETARIA REQUISITANTE	19.AGENTE DE PLANEJAMENTO	20.AUTORIZAÇÃO DA COMISSÃO
ASSINATURA E CARIMBO	Mariane A. C. Martins Agente de Planejamento ASSINATURA E CARIMBO	ASSINATURA E CARIMBO

21. AUTORIZAÇÃO DO PREFEITO

Instruções:

1.Nº: Numeração sequencial. 2.Unidade Requisitante: Sigla que identifica a Unidade Requisitante. 3.Data de Emissão. 4.Órgão Destino: Órgão/Secretaria para onde o documento será remetido. 5.Necessidade: Objeto da Requisição. 6.Justificativa: Motivação do pedido. 7.Vigência Contratual: Duração do contrato, convênio ou afim. 8.Informações Orçamentária/Financeira: Dotação orç., fonte de recurso e disponibiliadde financeira. 9.Forma de Pagamento: Discriminar o n.º de parcelas, o prazo e outros informações pertinentes. 10.Prazo/Local de Entrega: Indicar o prazo e local da entrega do bem, obra ou serviço. 11.Item: Seqüência numérica. 12.Código: Identificação do item no catálogo de compras. 13.Discriminação: Especificações do item. 14.Unid.: Unidade de medida. Ex.: resma, litros, quilos, etc. 15.QTD.: Quantidade desejada. 16.Valores: Valor unitário e total por item. 17.Valor Total Estimado: Valor estimado do pedido. 18.Requisitante: Assinatura e carimbo do(a) Secretário(a). 19.Agente de Planejamento:Assinatura e carimbo do Agente de Planejamento. 20. Autorização da Comissão: Campo destinado à autorização da CAOF. 21. Autorização do Prefeito: Assinatura e carimbo do Prefeito

ESTADO DA BAHIA

PREFEITURA MUNICIPAL DE ALAGOINHAS

PRAÇA GRACILIANO DE FREITAS, 1 - CENTRO
Alagoinhas - BA
C.N.P.J.: 13.646.005/0001-38

Solicitação / Reserva de Dotação

MAIO/2022

Tipo: Demais Processos | **Situação:** Aprovada

SOLICITANTE

Órgão: 30300 - SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO
Responsável: LUIZ CARLOS BASTOS PRATA
Cadastrado por: Mariane Almeida Costa Martins
Aprovado por: Patrícia de Santana Ferreira
Ped. Compra: Não

SD Nº: 618 / 2022
Data: 27/05/2022
Reservado: 27.750,00
Processo: 6600/2022
Reg. de Preço: Não

CLASSIFICAÇÃO

Órgão:	30300	SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO
Unid. Orçamentária:	030303	SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO
Função:	04	Administração
SubFunção:	126	Tecnologia da Informação
Programa:	0013	GESTÃO E MANUTENÇÃO DO PODER EXECUTIVO
Ação:	2196	MANUTENÇÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Natureza de Despesa:	33904000	Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica
SubElemento:		
Fonte:	15000000	Recursos não Vinculados de Impostos
Centro Custo:		
Base Legal:		

Objeto: Adesão a ata 93/2021 - TJTO, referente ao pregão eletrônico nº 39/2021 para contratação de empresa para a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – versão business select, incluindo atualizações e suporte técnico.

Justificativa: A Solução se caracteriza por garantir a segurança de computadores desktop, servidores e notebooks, assim como a proteção dos serviços e sistemas providos por esta administração.
Partimos da premissa de que o ambiente computacional da Prefeitura Municipal de Alagoinhas e suas diversas secretarias devem estar tecnologicamente atualizado, a fim de atender as demandas relativas à necessidade de segurança cibernética.
Diante disso, solicitamos a Adesão da Ata de Registro de Preços nº 39/2021 do Tribunal de Justiça do Estado do Tocantins.

Produto/Serviço	Und.	Qtd.	Estimado	Total
20642 - Licença de uso de software antivírus de rede, incluindo instalação e suporte. Contratação de empresa para aquisição de licença de uso de software antivírus de rede, incluindo instalação e suporte	UND	1,00	27.750,00	27.750,00

Valor Reservado: **27.750,00**

LUIZ CARLOS BASTOS PRATA
SECRETÁRIO DE ADMINISTRAÇÃO Mat.194751

Essa despesa foi devidamente reservada

Autorizo a solicitação da despesa

Solicitada: 27/05/2022 **Aprovada** 27/05/2022

ESTADO DA BAHIA
PREFEITURA MUNICIPAL DE ALAGOINHAS
SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO – SEMAD
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO - DTI

JUSTIFICATIVA DE ADESÃO DE ATA DE REGISTRO DE PREÇO

Ref.: Adesão à Ata de Registro de Preços Nº 93/2021 – PRESIDÊNCIA / DIGER / DIADM / DCC do Tribunal de Justiça do Estado do Tocantins

Pregão Eletrônico – SRP Nº 39/2021 - TJTO

Validade da Ata: 12 (doze) meses

DESCRIÇÃO: ADESÃO A ATA 93/2021 - TJTO, REFERENTE AO PREGÃO ELETRÔNICO 39/2021 PARA CONTRATAÇÃO DE EMPRESA PARA A AQUISIÇÃO DE LICENÇA DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS KASPERSKY ENDPOINT SECURITY – VERSÃO BUSINESS SELECT, INCLUINDO ATUALIZAÇÕES E SUPORTE TÉCNICO

As diversas secretarias da Prefeitura Municipal de Alagoinhas necessitam adquirir SOLUÇÃO DE LICENÇA PARA PROTEÇÃO CONTRA VÍRUS (ANTIVIRUS).

No intuito de acelerar a aquisição em questão, foram realizadas consultas a atas de registro de preços vigentes constantes no sítio de Compras Governamentais (Comprasnet), sendo identificado o pregão **SRP Nº 39/2021** realizado pelo órgão **Tribunal de Justiça do Estado do Tocantins (TJTO)** no qual a empresa **QUALITEK TECNOLOGIA - LTDA,** pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 10.224.281/0001-10, com sede à Rua José Ribeiro Dantas, 275, SL 404 e 406, Lagoa Nova, Natal/RN, foi vencedora do item "**2. Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select, com vigência de 36 (trinta e seis) meses**" cujas especificações atendem a necessidade da Prefeitura Municipal de Alagoinhas.

Foi realizada pesquisa de preços por esta diretoria, verificando-se que os valores propostos são superiores ao valor registrado na ARP em questão, ficando demonstrada que a aquisição através de adesão ao registro de preços do **TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS** é vantajosa para a Administração, gerando economia para a instituição e, diante disto, justifica-se a Adesão ao Registro de Preços do citado órgão.

Ademais, foi verificado que as especificações técnicas do(s) produto(s) constante(s) nos orçamentos estão de acordo com as especificações do(s) produto (s) que a Prefeitura Municipal de Alagoinhas pretende adquirir, conforme discriminado no termo de referência e ata de registro de preços do órgão gerenciado, em anexo.

Diante dos pressupostos acima, foi encaminhado ofícios solicitando adesão à Ata de Registro de Preços para a empresa Qualitek Tecnologia - LTDA, bem como ao Tribunal de Justiça do Estado do Tocantins, no qual foi autorizado a esta administração pública a adesão da mesma, conforme Ofícios nº 011/2022 e nº 012/2022 com as respectivas respostas em anexo.

Justificamos ainda que a adesão a Ata de Registro de Preços cumpre os princípios da vantajosidade, economicidade, eficácia e eficiência, uma vez que com este procedimento, a Prefeitura Municipal de Alagoinhas ADQUIRE UM PRODUTO OU CONTRATA UM SERVIÇO já aceito por outro Órgão Federal, fator que propicia segurança de que o material adquirido atenderá a demanda da Prefeitura Municipal de Alagoinhas, além de proporcionar presteza, celeridade e pronto atendimento à demanda dessa Instituição.

Diante disso, com fulcro no Decreto nº 7.892/2013, alterado pelo Decreto nº 9.488/2018, o modo escolhido para a aquisição da solução em epígrafe, foi à adesão à Ata de Registro de Preços nº 93/2021 do TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS, uma vez que este procedimento gerará economicidade e celeridade processual para a Prefeitura Municipal de Alagoinhas.

Atenciosamente,

Luiz Carlos Bastos Prata
Secretário Municipal da Administração

Anderson Ramos dos Santos
Diretoria de Tecnologia da Informação

Nº do Processo: 73/2021

Processo Finalizado

Licenciamento de direitos de uso de softwares para atender a Prefeitura de Piúma (Office Standard, Creative Cloud Adobe, CorelDraw, Kaspersky, Windows Server Datacenter 2019 e CALLs de acesso.)

Prefeitura Municipal de Piúma

Pregão Eletrônico

Exclusivo ME

DOCUMENTOS | IR PARA OS ITENS | ANDAMENTO DO PROCESSO

Informações

Tipo:

Pregão Eletrônico - Menor Preço

Tratamento da Fase de Lances:

Aberto

Operação:

Fechado p/ Operação

Pregoeiro:

Fernanda da Silva Pereira Parente

Autoridade Competente:

PAULO CELSO COLA PEREIRA

Apoio:

ANTONIO ALFREDO DE ANGELIS, DEBORA DIAS DA CONCEIÇÃO ALMEIDA, SELMA LUCIA DE ABREU NASCIMENTO,

Origem dos Recursos:

Próprio

Aplicar o Decreto 10.024/2019:

Não

Datas

Data de Abertura:

10/01/2022 às 13:00

Recebimento de Propostas:

29/12/2021 às 13:00 até 10/01/2022 às 12:59

Limite para Impugnações:

05/01/2022 às 13:00

CADASTRE-SE | FAZER LOGIN

PORTAL
DE COMPRAS PÚBLICAS

Documentos

Buscar documento

Documentos do Processo

Ata de Propostas

Documento

Baixar arquivo

Ata Parcial

Documento

Baixar arquivo

Ata Final

Documento

Lote 7 Registros

Buscar nos itens

1 - LICENÇA ZOOM MEETING CORPORATIVO PARA ATÉ 300 PARTICIPANTES 36 MESES - licenciamento com duração de 36 meses: disponibilizar a versão mais atual do produto na data da entrega do produto.- licenciamento para instituição tipo governo sediada no brasil.

Item
0002

Descrição
ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.

Unidade
UN

Quantidade
14

Melhor Lance
R$ 47.400,00

Valor Referência
R$ 180,00

Disputa
Exclusivo Micro Empresa

Situação
Homologado

Item
0005

Descrição
ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.

Unidade
UN

Quantidade
4

Melhor Lance
R$ 47.400,00

Valor Referência
R$ 180,00

Disputa
Exclusivo Micro Empresa

Situação
Homologado

Item
0010

Descrição
ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.

Unidade
UN

Quantidade
8

Melhor Lance
R$ 47.400,00

Valor Referência
R$ 180,00

Disputa
Exclusivo Micro Empresa

Situação
Homologado

ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.

Unidade
UN

Quantidade
6

Melhor Lance
R$ 47.400,00

Valor Referência
R$ 180,00

Disputa
ME Exclusivo Micro Empresa

Situação
Homologado

Item
0016

Descrição
ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.

Unidade
UN

Quantidade
8

Melhor Lance
R$ 47.400,00

Valor Referência
R$ 180,00

Disputa
ME Exclusivo Micro Empresa

Situação
Homologado

Item
0019

Descrição
ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.

Unidade
UN

Quantidade
50

Melhor Lance
R$ 47.400,00

Valor Referência
R$ 180,00

Disputa
ME Exclusivo Micro Empresa

Situação
Homologado

ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.

Unidade
UN

Quantidade
70

Melhor Lance
R$ 47.400,00

Valor Referência
R$ 180,00

Disputa
ME Exclusivo Micro Empresa

Situação
Homologado

Item
0025

Descrição
ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.

Unidade
UN

Quantidade
30

Melhor Lance
R$ 47.400,00

Valor Referência
R$ 180,00

Disputa
ME Exclusivo Micro Empresa

Situação
Homologado

ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.

Unidade
UN

Quantidade
100

Melhor Lance
R$ 47.400,00

Valor Referência
R$ 180,00

Disputa
ME Exclusivo Micro Empresa

Situação
Homologado

Item
0033

Descrição
ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.

Unidade
UN

Quantidade
10

Melhor Lance
R$ 47.400,00

Valor Referência
R$ 180,00

Disputa
ME Exclusivo Micro Empresa

Situação
Homologado

---

3 - AQUISIÇÃO DE CALS DE ACESSO PARA WINDOWS SERVER DATACENTER CORE 2019 - licença perpétua por equipamento- licenciamento para instituição tipo governo sediada no brasil

EFICIÊNCIA EM SERVIÇOS DE TI

2022

PROPOSTA COMERCIAL

KASPERSKY ENDPOINT SECURITY BUSINESS

Município de Alagoinhas

Anderson Ramos
(075) 9985-4998 r.7
ddi@alagoinha.ba.gov.br

Proposta: AIM708690/22Tc_1

1. APRESENTAÇÃO

A AIM7 é uma empresa que oferece diversas soluções para a área de tecnologia e segurança da informação. Fundada há 13 anos por profissionais com mais de 25 anos de experiência no setor, nos orgulhamos de basear nossa missão e valores na **excelência no atendimento aos nossos clientes**.

Desenvolvemos, para isso, um rico portfólio de serviços relacionados à produtos renomados, **e nosso time de analistas é altamente qualificado**, apto a oferecer um atendimento completo, auxiliando no plano de continuidade do seu negócio com os seguintes benefícios:

- Redução de Custos
- Qualidade Técnica
- Mobilidade
- Flexibilidade
- Escalabilidade
- Capacitação Profissional

AIM7 Serviços Gerenciados

AIM7 FIREWALL

Gestão completa da solução de Firewall com opção de locação do equipamento (appliance).

AIM7 BACKUP

Solução de Backup e Recovery mais rápida do mercado com o nosso serviço gerenciado para que sua empresa não corra mais o risco de perda de informação.

AIM7 ANTIVÍRUS

Tenha a solução anti-malware mais consagrada do mercado como serviço, com o nosso serviço de gestão incluso contemplando: instalação, atualização e gerenciamento completo.

AIM7 CLOUD ANTISPAM

Proteção completa contra SPAM e demais ameaças como Phishing e Ransomware, com o nosso serviço de gestão incluso.

AIM7 Serviços Profissionais

✓ **CONSULTORIA**
Fornecemos consultoria especializada na área de TI, com foco em Segurança da Informação.

✓ **SUPORTE TÉCNICO**
Atuarmos na resolução de incidentes que possam ocorrer durante a utilização de soluções de tecnologia.

- **IMPLEMENTAÇÃO**

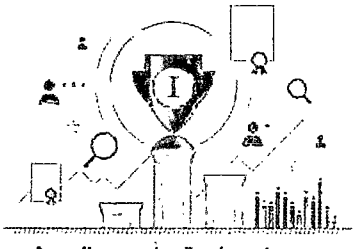
Implantar qualquer projeto de TI exige cuidados e muito planejamento, por isso conte com a AIM7 para estar ao seu lado em todo processo.

✓ **TREINAMENTO**
Desenvolva o potencial da sua equipe técnica com a nossa linha de treinamentos.

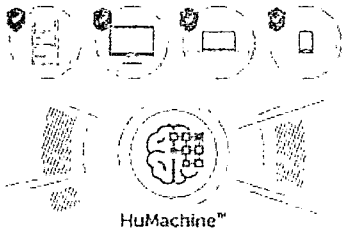
✓ **DIAGNÓSTICO**
Nosso serviço de Health Check ajuda a encontrar vulnerabilidades nas configurações que podem comprometer a segurança do seu negócio.

2. SOLUÇÃO KASPERSKY

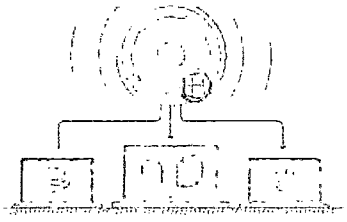
QUAL A SOLUÇÃO DE SEGURANÇA IDEAL PARA SUA EMPRESA?



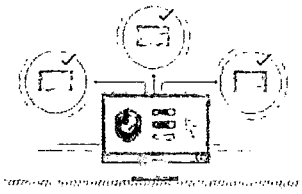
A melhor proteção do setor



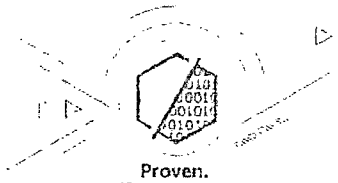
Segurança e controle completos para ambientes de TI mistos



Proteção além dos endpoints

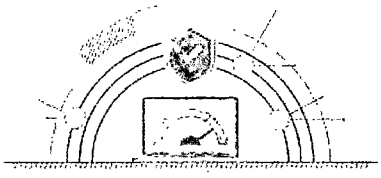


Um único produto da próxima geração, sem custos ocultos



Proven.
Transparent.
Independent.

Abertura que nenhum outro fornecedor oferece



Segurança adaptativa ágil

	Select SAIBA MAIS	Advanced	Total SAIBA MAIS
Segurança para computadores, Linux e Mac	✓	✓	✓
Segurança para servidores	✓	✓	✓
Segurança para dispositivos móveis	✓	✓	✓
Controle de Aplicativos para computadoress	✓	✓	✓
Controles de dispositivos e da Web	✓	✓	✓
Gerenciamento de mobilidade	✓	✓	✓
Controle de acesso baseado em função*		✓	✓
Gerenciamento de criptografia		✓	✓
Gerenciamento de correções e vulnerabilidades		✓	✓
Instalação de sistema operacional e software de terceiros		✓	✓
Controle de Aplicativos para servidores		✓	✓
Segurança para gateways da Web			✓
Segurança para servidores de e-mail			✓
Proteção contra ransomware	✓	✓	✓
Inteligência assistida por nuvem	✓	✓	✓
Console de gerenciamento único	✓	✓	✓
Integração com sistemas SIEM		✓	✓

3. VALORES

PRODUTOS

Item	Período	Partnumber	Descrição	Qtde	Valor Unitário	Valor Total
A	03 ANOS	KL4863KASLC	KESB Select Range: 150 a 249 licenças - Nova	250	R$ 202,27	R$ 50.567,50

RELAÇÃO CUSTO X BENEFÍCIO

Periodicidade	Valor Total	Custo Anual Total	Custo Anual por Máquina	Custo Mensal Total	Custo Mensal por Máquina
03 ANOS	R$ 50.567,50	R$ 16.855,83	R$ 67,42	R$ 1.404,65	R$ 5,62

Os cálculos acima são somente um estudo. Caso deseje contratar a solução com pagamento mensalizado, solicite proposta adequada ao seu vendedor.

5. CONDIÇÕES COMERCIAIS

- **As condições abaixo só serão válidas mediante aprovação de crédito.**
- Prazos de Pagamento:
  - Produto:
    10 DDL;
  - Serviços:
    Contrato de suporte anual e gestão: todo dia 10 de cada mês, consecutivamente, após aprovação desta proposta e, quando houver, da assinatura do contrato. Contrato de outsourcing: 1ª mensalidade no ato da assinatura do contrato (mediante análise de crédito) e aprovação desta proposta, com vencimento em 10 ddl, demais mensalidades após a instalação, com vencimento todo dia 10 de cada mês. Serviço Especializado ou Avulso: 10 ddl após a aprovação desta proposta.
- Forma de pagamento: Depósito
- Moedas
  - Valores expressos em USD serão convertidos pelo dólar comercial VENDA na data do faturamento.
  - Valores expressos em Real serão mantidos até seu faturamento.
- Validade da Proposta: 7 dias
- Prazo para início dos serviços: a combinar
- Impostos: Os preços incluem todo tipo de impostos e taxas (ICMS, IPI e Impostos de Importação, calculados pelas alíquotas atualmente vigentes). Os preços desta oferta serão alterados no caso de criação de novos tributos ou modificações das atuais alíquotas ou base de cálculo de impostos, bem como da ocorrência de mudanças fiscais ou cambiais resultantes de medidas governamentais.

6. INFORMAÇÕES ADICIONAIS

7. OBSERVAÇÕES

7.1. Os produtos (softwares e hardwares) serão faturados através de um de nossos fornecedores autorizados através de Faturamento Direto. Caso sua empresa emita Ordem de Compra, informe sua vendedora no ato do fechamento, para que possamos enviar os dados da empresa que emitirá Nota Fiscal e boleto.

7.2. Os serviços serão faturados pela AIM7, salvo observação explícita na proposta.

7.3. Todo e qualquer serviço adicional e não previsto nesta proposta será cobrado à parte, a ser negociado através de proposta comercial prévia.

7.4. Licenças de software são comercializadas somente via download, não existindo caixas de produtos, manuais ou mídias de instalação. Toda documentação necessária é enviada por e-mail, inclusive as chaves de ativação dos produtos adquiridos.

8. CONFIDENCIALIDADE

Todas as informações contidas neste documento são consideradas de uso restrito de ambas as partes envolvidas e citadas neste documento. Este material inclui informações consideradas sigilosas e a sua divulgação só deverá ser praticada com a finalidade especifica de avaliação de seu conteúdo para a aprovação e contratação destes serviços. Sendo assim, é proibida a reprodução de partes ou de todo o conteúdo, por quaisquer meios, sem a autorização forma das partes envolvidas.

Ficamos à inteira disposição para quaisquer esclarecimentos adicionais.

Atenciosamente,

Tom Cordeiro

Gerente de Contas
PABX +55 11-2076-4545 - ramal 2005
E-mail: tom.cordeiro@aim7.com.br

VENCEDORES DO PROCESSO

Prefeitura Municipal de Piúma
Prefeitura Municipal de Piúma
Pregão Eletrônico - 73/2021

4F SOLUCOES EM TECNOLOGIA LTDA - Tipo: EPP/SS - LC123: Sim - Documento 30.357.688/0001-22 - Endereço: SRTVS - CEP: 70340000 - UF: DF - Município: - Telefone: (61) 3037-2006

Lote	Item	Produto	Modelo	Marca/ Fabricante	Melhor Lance	Valor Total
0002		ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - licenciamento com duração de 36 meses: disponibilizar a versão mais atual do produto na data da entrega do produto.- licenciamento para instituição tipo governo sediada no brasil.				
	0002	ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.	N/C	N/C	158,00	2.212,00
	0005	ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.	N/C	N/C	158,00	632,00
	0010	ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.	N/C	N/C	158,00	1.264,00
	0013	ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.	N/C	N/C	158,00	948,00
	0016	ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.	N/C	N/C	158,00	1.264,00
	0019	ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.	N/C	N/C	158,00	7.900,00
	0022	ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.	N/C	N/C	158,00	11.060,00

	0025	ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.	N/C	N/C	158,00	4.740,00
	0028	ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.	N/C	N/C	158,00	15.800,00
	0033	ANTIVIRUS KASPERSKY ENDPOIND SECURITY FOR BUSSINESS - Licenciamento com duração de 36 meses: Disponibilizar a versão mais atual do produto na data da entrega do produto.- Licenciamento para instituição tipo Governo sediada no Brasil.	N/C	N/C	158,00	1.580,00
		TOTAL DO LOTE				R$ 47.400,00
					TOTAL DO VENCEDOR	R$ 47.400,00

ABR INFORMATICA PECAS E SERVICOS EIRELI - Tipo: Ltda/Eireli - LC123: Sim - Documento 27.218.328/0001-35 - Endereço: SHCES Quadra 605 Bloco E - CEP: 70655655 - UF: DF - Município: - Telefone: (61) 9987-2879

Lote	Item	Produto	Modelo	Marca/ Fabricante	Melhor Lance	Valor Total
0004		CORELDRAW GRAPHICS SUITE 2021 - licença perpétua - licenciamento para instituição tipo governo sediada no brasil				
	0009	CORELDRAW GRAPHICS SUITE 2021 - Licença Perpétua - Licenciamento para instituição tipo Governo sediada no Brasil	N/C	N/C	2.758,00	13.790,00
		TOTAL DO LOTE				R$ 13.790,00
					TOTAL DO VENCEDOR	R$ 13.790,00

JOAO PAULO DE SOUSA SILVA 04768313345 - Tipo: Ltda/Eireli - LC123: Sim - Documento 37.625.496/0001-07 - Endereço: Quadra 3 Casa 29 - CEP: 64082003 - UF: PI - Município: - Telefone: (86) 98853-1395

Lote	Item	Produto	Modelo	Marca/ Fabricante	Melhor Lance	Valor Total
0006		LICENÇA PERPÉTUA PARA SISTEMA OPERACIONAL WINDOWS SERVER DATA CENTER 2019 compatível com equipamento ibm x3750 m4 (8722ac1) processador xeon ® cpu e-5-4610 2.40 ghz (4 processadores)				
	0029	LICENÇA PERPÉTUA PARA SISTEMA OPERACIONAL WINDOWS SERVER DATA CENTER 2019 Compatível com Equipamento IBM X3750 M4 (8722AC1) Processador XEON ® CPU E-5-4610 2.40 GHz (4 Processadores)	N/C	N/C	6.700,00	13.400,00
		TOTAL DO LOTE				R$ 13.400,00
					TOTAL DO VENCEDOR	R$ 13.400,00

Valor Total: R$ 74.590,00

ESTADO DA BAHIA
PREFEITURA MUNICIPAL DE ALAGOINHAS
SECRETARIA MUNICIPAL DA ADMINISTRAÇÃO

Alagoinhas-Bahia, 26 de abril de 2022

Oficio nº 012/2022

Ao **Tribunal de Justiça do Estado do Tocantins**
Praça dos Girassóis, s/nº, Centro, Palmas/TO CEP: 77.015-007
Ac. Sr. Desembargador João Rigo Guimarães – Presidente
Ref.: Ata de Registro de Preços Nº 93/2021 - PRESIDÊNCIA/DIGER/DIADM/DCC

A Secretaria Municipal da Administração (SEMAD) da Prefeitura Municipal de Alagoinhas – Bahia solicita autorização ao Tribunal de Justiça do Estado do Tocantins para aderir à Ata de Registro de Preços nº 93/2021, oriunda do Pregão Eletrônico N° 39/2021 e em conformidade com os limites e valores registrados na respectiva Ata. Para tanto informamos o número dos itens da Ata que temos interesse em adquirir como órgão interessado e suas respectivas quantidades:

Item	Descrição	Valor Unit	Qtd	Valor Total
2	Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select, com vigência de 36 (trinta e seis) meses.	R$ 111,00	250	R$ 27.750,00

Atenciosamente,

Luiz Carlos Bastos Prata
Secretário Municipal da Administração (SEMAD)

Anderson Ramos dos Santos
Diretor de Tecnologia da Informação / SEMAD

Contatos do servidor (Diretor de Tecnologia):
Telefone: 75 98328-0683 – E-mail: dti@alagoinhas.ba.gov.br
Horário de Funcionamento: Das 7h às 13h.

Assunto: **Solicitação de Autorização para Adesão à Ata de Registro de Preços nº 93/2021 TJ-TO**

De <dti@alagoinhas.ba.gov.br>

Para: <spadg@tjto.jus.br>

Cc: Anderson Ramos dos Santos DTI <aramos@alagoinhas.ba.gov.br>, Paulo Lopes - SECRI <plopes@alagoinhas.ba.gov.br>, Diretoria Administrativa e Financeira SEMAD <daf.semad@alagoinhas.ba.gov.br>, Glauberter Nadson DTI <gnsilva@alagoinhas.ba.gov.br>

Data 27/04/2022 10:28

- Ofício 012-2022 - Solicitação de Adesão ao TJTO.pdf (~556 KB)

Prezados(as), bom dia.

Cordialmente cumprimentando-os, viemos por meio deste, enviar Ofício referente à Solicitação de Autorização para Adesão à Ata de Registro de Preços nº 93/2021 - PRESIDÊNCIA/DIGER/DIADM/DCC, conforme documento em anexo.

Salientamos que estamos enviando também ofício para a empresa contratada (Qualitek) quanto à esta solicitação.

No ensejo, estamos à disposição para maiores esclarecimentos quanto à solicitação e documentos que forem necessários para envio.

Agradecemos antecipadamente e muito apreço.

Atenciosamente,

Anderson Ramos dos Santos

Diretor de Tecnologia da Informação

Secretaria Municipal da Administração

Prefeitura Municipal de Alagoinhas

Assunto: **Adesão a Ata de Registro de Preços**

De TJ-TO/e-mail da SPADG <spadg@tjto.jus.br>

Para: <dti@alagoinhas.ba.gov.br>

Data 24/05/2022 14:19

Prioridade Normal

- Ata de Registro de Preços nº93 - 1.pdf (~313 KB)
- Extrato de Publicação da Ata - 2.pdf (~167 KB)
- Edital COLIC - 3.pdf (~2.8 MB)
- Aviso de Licitação - publicação Diário da Justiça - 4.pdf (~167 KB)
- Ata da Sessão - 5.pdf (~85 KB)
- Parecer Jurídico ASJUADMDG - 6.pdf (~167 KB)
- Termo de Homologação - 7.pdf (~148 KB)
- Contrato nº 218 - 8.pdf (~666 KB)
- Extrato da Publicação do Contrato - 9.pdf (~255 KB)
- Planilha de controle de adesão - 10.pdf (~73 KB)
- Manifestação gestor - 11.pdf (~124 KB)
- Aceite do fornecedor - 12.pdf (~208 KB)
- Oficio_4337969.html (~33 KB)
- Despacho_4336702.html (~44 KB)
- Informacao_4331771.html (~50 KB)
- Despacho_4335099.html (~61 KB)

Encaminho o Ofício 3927 SPADG (evento 4337969) e seus anexos, para conhecimento.

OBS: Favor acusar o recebimento deste e-mail.

Secretaria de Processos Administrativos da Diretoria Geral - SPADG
Tribunal de Justiça do Estado do Tocantins
Telefone: (63) 3218-4308

Qualitek

Ofício nº 011/2022

Ao **Tribunal de Justiça do Tocantins**
Ac.: DIADM/TJ-TO

A Qualitek Tecnologia Ltda, inscrita sob CNPJ 10.224.281/0001-10, serve do presente para confirmar a aceitação para que a Prefeitura Municipal de Alagoinhas (Bahia), faça adesão da Ata de registro de preço nº 93/2021 e pregão eletrônico nº 39/2021 do Tribunal de Justiça do Tocantins, com valor global de R$ 27.750,00 conforme quantidades e itens listados abaixo. Ainda declaramos à ausência de prejuízo do compromisso assumido na respectiva Ata, bem como observância do quantitativo solicitado por meio do referido Ofício nº 012/2022.

Item	Descrições	Qtd	Valor Unitário	Valor Total
2	Aquisição de licenças do software de antivírus Kaspersky Endpoint Security- Versão Business Select, com vigência de 36 (trinta e seis) meses.	250	R$ 111,00	R$ 27.750,00
			Total	**R$ 27.750,00**

Natal, 13 de maio de 2022

DENNIS FERNANDES DE MEDEIROS
Sócio-Diretor Comercial

Zimbra **diadm@tjto.jus.br**

Re: Adesão a ARP nº 93/2021

De : Dennis Fernandes <dennis.fernandes@qualitek.com.br> sex, 13 de mai de 2022 12:25
1 anexo

Assunto : Re: Adesão a ARP nº 93/2021

Para : TJ-TO/Diretoria Administrativa <diadm@tjto.jus.br>, Marla Sales <marla.sales@qualitek.com.br>

Cc : Qualitek Tecnologia <tecnologia@qualitek.com.br>

As imagens externas não são exibidas. Exibir as imagens abaixo

Pezada Aldeni, boa tarde!

Segue em anexo nosso aceite quanto a solicitação da Prefeitura Municipal de Alagoinhas (Bahia).

Ficamos à disposição.

Atenciosamente,

On Fri, May 13, 2022 at 12:16 PM TJ-TO/Diretoria Administrativa <diadm@tjto.jus.br> wrote:

> Boa Tarde!
>
> A/C : Senhor Dennis Fernandes de Medeiros, representante da empresa: Qualitek Tecnologia - Ltda.
>
> De ordem, informo que à Secretaria Municipal da Administração da Prefeitura Municipal de Alagoinhas-Bahia, tem interesse em adquirir produtos dessa empresa, nos termos do Ofício nº 012/2022/, em anexo.
>
> Assim, solicito manifestação dessa empresa quanto ao interesse em fornecer os produtos à Secretaria Municipal da Administração da Prefeitura Municipal de Alagoinhas-Bahia, desde que condicionada à ausência de prejuízo do compromisso assumido na respectiva Ata, bem como observância do quantitativo solicitado por meio do referido Ofício nº 012/2022.
>
> Atenciosamente,
>
> Aldeni Brites de Souza
> Assistente Administrativo
> DIADM/TJ-TO
> Fone: 3218-4283
>
> Palmas,13 de maio de 2022.

--
Dennis Fernandes
Qualitek Tecnologia
Diretor Comercial
Cel: +55 (84) 9 9113-6771 | (84) 9 8118-0758 (WhatsApp)
www.qualitek.com.br

Qualitek - Oficio 011_2022 - TJTO.pdf
128 KB

ESTADO DA BAHIA
PREFEITURA MUNICIPAL DE ALAGOINHAS
SECRETARIA MUNICIPAL DA ADMINISTRAÇÃO

Alagoinhas-Bahia, 26 de abril de 2022

Oficio nº 011/2022

Á Qualitek Tecnologia Ltda
Ac. Sr. Dennis Fernandes de Medeiros – Diretor Comercial
Email: Tecnologia@qualitek.com.br, Telefone: 84-4008-9454
Endereço: Rua José Ribeiro Dantas, 275, Salas 404 e 406, Lagoa Nova - Natal/RN - CEP: 59062-480
Ref.: Ata de Registro de Preços Nº 93/2021 - PRESIDÊNCIA/DIGER/DIADM/DCC

Demonstramos interesse em aderir a Ata de Registro de Preços nº 93/2021, Pregão Eletrônico Nº 39/2021 do Tribunal de Justiça do Tocantins em que a Qualitek é o fornecedor conforme descrito e quantificado a seguir:

Item	Descrição	Valor Unit	Qtd	Valor Total
2	Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select, com vigência de 36 (trinta e seis) meses.	R$ 111,00	250	R$ 27.750,00

Formulamos consulta ao Tribunal de Justiça do Estado de Tocantins acerca da possibilidade desta adesão.

Atenciosamente,

Luiz Carlos Bastos Prata
Secretário Municipal da Administração (SEMAD)

Anderson Ramos dos Santos
Diretor de Tecnologia da Informação / SEMAD

Contatos do servidor (Diretor de Tecnologia):
Telefone: 75 98328-0683 – E-mail: dti@alagoinhas.ba.gov.br
Horário de Funcionamento: Das 7h às 13h.

Assunto:	**Solicitação de Adesão à Ata de Registro de Preços nº 93/2021 TJ-TO**
De	<dti@alagoinhas.ba.gov.br>
Para:	<tecnologia@qualitek.com.br>
Cc:	Anderson Ramos dos Santos DTI <aramos@alagoinhas.ba.gov.br>, <daf.semad@alagoinhas.ba.gov.br>, Glauberter Nadson DTI <gnsilva@alagoinhas.ba.gov.br>, Paulo Lopes - SECRI <plopes@alagoinhas.ba.gov.br>
Data	27/04/2022 10:22

- Ofício 011-2022 - Solicitação de Adesão a Qualitek.pdf (~549 KB)

Prezados(as), bom dia.

Cordialmente cumprimentando-os, viemos por meio deste enviar Ofício referente à Solicitação para Adesão à Ata de Registro de Preços nº 93/2021 - PRESIDÊNCIA/DIGER/DIADM/DCC, conforme documento em anexo.

Salientamos que estamos enviando também ofício para o TJ-TO quanto à esta solicitação.

No ensejo, estamos à disposição para maiores esclarecimentos quanto à solicitação e documentos que forem necessários para envio.

Agradecemos antecipadamente e muito apreço.

Atenciosamente,

Anderson Ramos dos Santos

Diretor de Tecnologia da Informação

Secretaria Municipal da Administração

Prefeitura Municipal de Alagoinhas

Assunto:	**RES: Solicitação de Adesão à Ata de Registro de Preços nº 93/2021 TJ-TO**
De	Marla Sales <marla.sales@qualitek.com.br>
Para:	<dti@alagoinhas.ba.gov.br>
Cc:	'Anderson Ramos dos Santos DTI' <aramos@alagoinhas.ba.gov.br>, <daf.semad@alagoinhas.ba.gov.br>, 'Glauberter Nadson DTI' <gnsilva@alagoinhas.ba.gov.br>, 'Paulo Lopes - SECRI' <plopes@alagoinhas.ba.gov.br>, <dennis.fernandes@qualitek.com.br>
Responder para	<marla.sales@qualitek.com.br>
Data	27/04/2022 15:20

- Qualitek - Oficio 10_2022 - Pref.M.Alagoinhas.pdf (~540 KB)

Boa tarde!

Em anexo resposta positiva a solicitação em oficio

Ficamos a disposição

Sds,
Marla Sales
Comercial
84.4008-9454/ 84 9.9949-3544(WhatsApp)
WWW.qualitek.com.br

qualitektecnologia | www.qualitek.com.br

Acesse todos os Webinars promovidos pela Qualitek acessando:
https://www.gotostage.com/channel/bf5a333279484e7b881a7621ba662846

De: dti@alagoinhas.ba.gov.br [mailto:dti@alagoinhas.ba.gov.br]
Enviada em: quarta-feira, 27 de abril de 2022 10:22
Para: tecnologia@qualitek.com.br
Cc: Anderson Ramos dos Santos DTI; daf.semad@alagoinhas.ba.gov.br; Glauberter Nadson DTI; Paulo Lopes - SECRI
Assunto: Solicitação de Adesão à Ata de Registro de Preços nº 93/2021 TJ-TO

Prezados(as), bom dia.

Cordialmente cumprimentando-os, viemos por meio deste enviar Ofício referente à Solicitação para Adesão à Ata de Registro de Preços nº 93/2021 - PRESIDÊNCIA/DIGER/DIADM/DCC, conforme documento em anexo.

Salientamos que estamos enviando também ofício para o TJ-TO quanto à esta solicitação.

No ensejo, estamos à disposição para maiores esclarecimentos quanto à solicitação e documentos que forem necessários para envio.

Agradecemos antecipadamente e muito apreço.

Atenciosamente,

Anderson Ramos dos Santos

Diretor de Tecnologia da Informação

Secretaria Municipal da Administração

Prefeitura Municipal de Alagoinhas

JUSTIFICATIVA TÉCNICA

OBJETO: CONTRATAÇÃO DE EMPRESA PARA A AQUISIÇÃO DE LICENÇA DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS KASPERSKY ENDPOINT SECURITY – VERSÃO BUSINESS SELECT, INCLUINDO ATUALIZAÇÕES E SUPORTE TÉCNICO.

Ao longo dos últimos anos, a Solução Corporativa de Antivírus tem contribuído para a integridade e disponibilidade da segurança da informação do ambiente computacional das diversas secretarias da Prefeitura Municipal de Alagoinhas, protegendo a rede corporativa de ataques de malwares originados da Internet e de dispositivos infectados, tal como pendrives.

A Solução se caracteriza por garantir a segurança de computadores desktop, servidores e notebooks, assim como a proteção dos serviços e sistemas providos por esta administração.

Partimos da premissa de que o ambiente computacional da Prefeitura Municipal de Alagoinhas e suas diversas secretarias devem estar tecnologicamente atualizado, a fim de atender as demandas relativas à necessidade de segurança cibernética.

Os recursos computacionais desta municipalidade utilizavam a Solução de Antivírus Licenciado da empresa Kaspersky. Contudo, com o término da garantia de atualização ocorrida em agosto de 2020, as licenças utilizadas não permitiram mais a atualização de novas versões da solução e das bases de dados (lista de vírus e vacinas), o que acarreta em vulnerabilidades na rede corporativa, assim como a possibilidade de entrada de malwares, como vírus e worms, capazes de comprometer a integridade e disponibilidade dos dispositivos computacionais desta municipalidade.

Desse modo, faz-se necessário adquirir uma solução de antivirus, para que a Prefeitura Municipal de Alagoinhas e suas diversas secretarias possam permanecer com a premissa de otimizar e promover a segurança da informação.

A aquisição de licenças de antivírus possui, como intuito, prevenir a contaminação por vírus, malwares, suas variantes e demais ameaças cibernéticas,

nas diversas tecnologias computacionais que podem pôr em risco o sigilo, a integridade e a disponibilidade das informações.

Devido à grande utilização de e-mails e acesso a páginas de internet, a aquisição de software de antivírus corporativo passa a ser necessária para fornecer segurança à infraestrutura de rede, computadores, servidores e notebooks, sendo este licenciamento imprescindível para os ambientes informatizados.

Estas aquisições buscam proporcionar maior proteção aos computadores das secretarias, resguardando problemas que possam prejudicar os serviços prestados aos cidadãos. Portanto, é uma questão de segurança, que possibilita garantir o desempenho das estações de trabalho e, por conseguinte, disponibilizar aos funcionários condições para a realização de suas atividades. A aquisição destas licenças é essencial para que estas tarefas sejam executadas com êxito.

Nesse contexto, a contratação faz-se necessária para assegurar a proteção do ambiente computacional do órgão público, desse modo é de extrema importância adquirir essa solução de antivírus licenciado para que a municipalidade possa permanecer com a premissa de otimizar e promover a segurança da informação.

Atenciosamente,

Anderson Ramos dos Santos
Diretor de Tecnologia da Informação

Ofício nº 3927 / 2022 - PRESIDÊNCIA/DIGER/SPADG

Palmas, 19 de maio de 2022.

A Sua Senhoria, Senhor
LUIZ CARLOS BASTOS PRATA
Secretário Municipal da Administração - BA
48007-656 - Alagoinhas BA
E-mail: dti@alagoinhas.ba.gov.br

Assunto: Adesão a Ata de Registro de Preços
Processo SEI nº 22.0.000011991-5

Senhor Secretário,

Em resposta ao solicitado por meio do Ofício nº 012/2022, comunico a autorização deste Tribunal de Justiça para adesão à Ata de Registro de Preços nº 93/2021, conforme Despacho DIGER 35117 (evento 4336702), tendo em vista a observância do disposto no art. 22 do Decreto Federal nº 7.892/2013, que versa sobre o quantitativo total, por órgão não participante, nas adesões solicitadas, aplicados junto a este Poder, corroborados por força do Decreto Judiciário nº 6 de 2020.

Observa-se a concordância da empresa **Qualitek Tecnologia - Ltda**, no entanto, vale ressaltar que devem ser seguidas as regras contidas no Edital de Licitação do Pregão Eletrônico - SRP nº 39/2021.

Oportunamente, oriento ao solicitante que envie ao Órgão gerenciador da Ata, cópia da Nota de Empenho assinada, após a assinatura do contrato com o fornecedor.

Atenciosamente,

sei! assinatura eletrônica

Documento assinado eletronicamente por **Jonas Demostene Ramos**, **Diretor Geral**, em 24/05/2022, às 13:49, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **4337969** e o código CRC **5306EEB4**.

PROCESSO 22.0.000011991-5
INTERESSADO Secretaria da Administração do Município de Alagoinhas /Bahia
ASSUNTO Solicitação e Adesão à ARP nº 93/2021, P. Eletrônico - SRP nº 39/2021

Informação Nº 17106 / 2022 - PRESIDÊNCIA/DIGER/DIADM/ASDIADM

Ao Diretor Administrativo

Cuidam os presentes autos de solicitação de adesão pela **Secretaria da Administração do Município de Alagoinhas-Bahia,** conforme expediente de evento 4292758, à Ata de Registro de Preços nº 93/2021, advinda do Pregão Eletrônico - SRP nº 39/2021, tendo por objeto o registro de preços visando à renovação e a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – Versão Business Select, incluindo atualizações e suporte técnico, com o objetivo de atender às demandas do Poder Judiciário do Estado do Tocantins, tendo como fornecedor registrado a empresa : Qualitek Tecnologia - Ltda, **CNPJ/MF:10.224.281/0001-10, Endereço:** Rua José Ribeiro Dantas, 275, SL 404 e 406, Lagoa Nova, CEP 59062-480, Natal/RN, Telefones: (84) 4008-9454, e-mail: : tecnologia@qualitek.com.br, sendo representante: Dennis Fernandes de Medeiros - portador do RG nº 2468043 - ITEP/RN, inscrito no CPF/MF nº 084.417.344-45, conforme SEI: 21.0.000002638-4 e 21.0.000020119-4, a estes relacionados.

Para instrução do feito, os autos vieram à esta Diretoria Administrativa conforme Despacho DIGER de evento 4298740, modo pelo qual solicitamos manifestação do gestor, nos termos do Despacho DIADM de evento 4301762.

O gestor da Ata em apreço, por sua vez, sinaliza favoravelmente à concessão da adesão ora pleiteada, nos termos dos eventos 4307403 e 4321529 respectivamente, corroborado pela Planilha de Controle de ARP de evento 4307247.

Via e-mail (evento 4324904), solicitamos ao representante da empresa manifestação quanto ao interesse em fornecer ao solicitante, tendo o representante se manifestado favoravelmente, conforme evento 4326736.

Oportunamente, sugerimos que os seguintes documentos dos presentes autos, bem assim, dos autos relacionados acompanhem o ofício autorizativo, quais sejam:

1. Ata de Registro de Preços nº93/2021 - evento 3857975;
2. Extrato de Publicação da Ata - evento 3857977;
3. Edital COLIC - evento 3776143;
4. Aviso de Licitação - publicação Diário da Justiça - evento 3855022;

5. Ata da Sessão - evento 3813934;

6. Parecer Jurídico ASJUADMDG - evento 3830849;

7. Termo de Homologação - evento 3830858;

8. Contrato nº 218/2021 - evento 3876515

9. Extrato da Publicação do Contrato - evento 3881861;

10. Planilha de controle de adesão - evento 4307247;

11. Manifestação gestor - evento 4307403.

12. Aceite do fornecedor - evento 4326736;

Registra-se que, considerando a Decisão nº 5302/2021, proferida no evento 4072065 dos autos 21.0.000028154-6, o órgão solicitante **não apresentou a justificativa** quanto à vantajosidade da adesão.

Desta feita, consoante Memorando nº 849/2020 e Despacho 58598/2020 (eventos 3094877 e 3381754), da Diretoria Administrativa, versando sobre os controles internos, informo que a instrução dos presentes autos está de acordo com o normativo interno pertinente, no tocante ao quantitativo total, por órgão não participante, nas adesões solicitadas, aplicados junto a este Poder, nos termos do art. 22 do Decreto Federal nº 7.892, de 2013, corroborado por força do Decreto Judiciário nº 6 de 2020, destacando-se a ausência da justificativa quanto à vantajosidade.

Nesta oportunidade, solicitamos ao órgão solicitante o envio de cópia da nota de empenho, após sua assinatura, a este Tribunal, para efeito de registro e baixa do saldo ora disponível.

Posto isto, submeto a presente Informação ao Diretor Administrativo para conhecimento, com sugestão de remessa à Diretoria Geral para deliberação.

Documento assinado eletronicamente por **Aldeni Brites de Souza**, **Assistente Administrativo**, em 18/05/2022, às 15:25, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **4331771** e o código CRC **6150ABF2**.

PROCESSO 22.0.000011991-5
INTERESSADO Secretário Municipal de Administração - Prefeitura Municipal de Alagoinhas - Bahia
ASSUNTO Solicitação de Adesão à ARP nº 93/2021, P. Eletrônico - SRP nº 39/2021

Despacho Nº 34882 / 2022 - PRESIDÊNCIA/DIGER/DIADM

Senhor Diretor Geral,

Cuida os presentes autos de solicitação de adesão pela **Secretaria Municipal da Administração da Prefeitura Municipal de Alagoinhas-Bahia**, conforme Ofício Nº 012/2022 (evento 4292758), à Ata de Registro de Preços Nº 93/2021, oriunda do Pregão Eletrônico Nº 39/2021 (evento 3843127), cujo o objeto do presente Instrumento é o registro de preços visando à contratação de empresa **Qualitek Tecnologia - Ltda; CNPJ/MF: 10.224.281/0001-10, Endereço:** Rua José Ribeiro Dantas, 275, SL 404 e 406, Lagoa Nova, CEP 59062-480, Natal/RN; **Telefone:** (84) 4008-9454; e-mail: *tecnologia@qualitek.com.br;* **Representante:** Dennis Fernandes de Medeiros - portador do RG nº 2468043 - ITEP/RN, inscrito no CPF/MF sob o nº 084.417.344-45, **Itens:** 1 e 2, conforme SEI: 21.0.000002638-4 e 21.0.000020119-4, a estes relacionados.

O gestor da Ata em apreço, por sua vez, sinaliza favoravelmente à concessão da adesão ora pleiteada, nos termos do evento 4307403 e 4321529, corroborado pela Planilha de Controle de ARP de evento 4307247.

A Informação ASDIADM de evento 4331771, traz a análise dos documentos, nos seguintes termos:

> Ao Diretor Administrativo
>
> Cuidam os presentes autos de solicitação de adesão pela **Secretaria da Administração do Município de Alagoinhas-Bahia,** conforme expediente de evento 4292758, à Ata de Registro de Preços nº 93/2021, advinda do Pregão Eletrônico - SRP nº 39/2021, tendo por objeto o registro de preços visando à renovação e a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – Versão Business Select, incluindo atualizações e suporte técnico, com o objetivo de atender às demandas do Poder Judiciário do Estado do Tocantins, tendo como fornecedor registrado a empresa : Qualitek Tecnologia - Ltda, **CNPJ/MF:10.224.281/0001-10, Endereço:** Rua José Ribeiro Dantas, 275, SL 404 e 406, Lagoa Nova, CEP 59062-480, Natal/RN, Telefones: (84) 4008-9454, e-mail: : tecnologia@qualitek.com.br, sendo representante: Dennis Fernandes de Medeiros - portador do RG nº 2468043 - ITEP/RN, inscrito no CPF/MF nº 084.417.344-45, conforme SEI: 21.0.000002638-4 e 21.0.000020119-4, a estes relacionados.
>
> Para instrução do feito, os autos vieram à esta Diretoria Administrativa conforme Despacho DIGER de evento 4298740, modo pelo qual solicitamos manifestação do gestor, nos termos do Despacho DIADM de evento 4301762.
>
> O gestor da Ata em apreço, por sua vez, sinaliza favoravelmente à concessão da adesão ora pleiteada, nos termos dos eventos 4307403 e 4321529 respectivamente, corroborado pela Planilha de Controle de ARP de evento 4307247.
>
> Via e-mail (evento 4324904), solicitamos ao representante da empresa manifestação quanto ao interesse em fornecer ao solicitante, tendo o representante se manifestado favoravelmente, conforme evento 4326736.

Oportunamente, sugerimos que os seguintes documentos dos presentes autos, bem assim, dos autos relacionados acompanhem o ofício autorizativo, quais sejam:

1. Ata de Registro de Preços nº93/2021 - evento 3857975;

2. Extrato de Publicação da Ata - evento 3857977;

3. Edital COLIC - evento 3776143;

4. Aviso de Licitação - publicação Diário da Justiça - evento 3855022;

5. Ata da Sessão - evento 3813934;

6. Parecer Jurídico ASJUADMDG - evento 3830849;

7. Termo de Homologação - evento 3830858;

8. Contrato nº 218/2021 - evento 3876515

9. Extrato da Publicação do Contrato - evento 3881861;

10. Planilha de controle de adesão - evento 4307247;

11. Manifestação gestor - evento 4307403.

12. Aceite do fornecedor - evento 4326736;

Registra-se que, considerando a Decisão nº 5302/2021, proferida no evento 4072065 dos autos 21.0.000028154-6, o órgão solicitante **não apresentou a justificativa** quanto à vantajosidade da adesão.

Desta feita, consoante Memorando nº 849/2020 e Despacho 58598/2020 (eventos 3094877 e 3381754), da Diretoria Administrativa, versando sobre os controles internos, informo que a instrução dos presentes autos está de acordo com o normativo interno pertinente, no tocante ao quantitativo total, por órgão não participante, nas adesões solicitadas, aplicados junto a este Poder, nos termos do art. 22 do Decreto Federal nº 7.892, de 2013, corroborado por força do Decreto Judiciário nº 6 de 2020, destacando-se a ausência da justificativa quanto à vantajosidade.

Nesta oportunidade, solicitamos ao órgão solicitante o envio de cópia da nota de empenho, após sua assinatura, a este Tribunal, para efeito de registro e baixa do saldo ora disponível.

Posto isto, submeto a presente Informação ao Diretor Administrativo para conhecimento, com sugestão de remessa à Diretoria Geral para deliberação.

Assim, em cumprimento ao Despacho DIGER nº 29690/2022 (evento 4298740), e considerando a Informação ASDIADM nº 17106/2022 (evento 4331771) em epígrafe, conforme os fundamentos e as informações apresentadas, retorno os autos à autoridade superior para deliberação, com sugestão de envio de expediente ao órgão solicitante.

Por fim, em caso de autorização, solicito que seja pleiteado ao órgão solicitante o envio de cópia da nota de empenho a este Tribunal (órgão gerenciador), para fins de registro e baixa do saldo disponibilizado, bem como sugiro que sejam remetidos os documentos licitatórios relacionados na Informação ASDIADM nº 17106/2022 (evento 4331771), os quais irão auxiliar na instrução dos autos do órgão solicitante.

Retorno à unidade gestora da ARP para conhecimento, com sugestão de acompanhamento.

Respeitosamente,

Documento assinado eletronicamente por **Ronilson Pereira da Silva, Diretor Administrativo**, em 18/05/2022, às 18:33, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **4335099** e o código CRC **19E051FD**.

PROCESSO 22.0.000011991-5
INTERESSADO Luiz Carlos Bastos Prata - Secretário Municipal de Administração, Anderson Ramos dos Santos - Diretor de Tecnologia da Informação, Prefeitura Municipal de Alagoinhas - Bahia
ASSUNTO Adesão a Ata de Registro de Preços

Despacho Nº 35117 / 2022 - PRESIDÊNCIA/DIGER

Cuidam os autos de solicitação de adesão pela Secretaria Municipal da Administração da Prefeitura Municipal de Alagoinhas-Bahia, para adesão à Ata de Registro de Preços nº 93//2021 oriunda do Pregão Eletrônico - SRP nº Nº 39/2021, cujo o objeto é o registro de preços visando à contratação de empresa **Qualitek Tecnologia - Ltda; CNPJ/MF: 10.224.281/0001-10**.

Instruídos os autos, acolho os termos do Despacho DIADM do evento 4335099 e **Autorizo** a adesão do item solicitado disponível, **ARP nº 93/2021 oriundo do Pregão Eletrônico - SRP nº 39/2021,** conforme demonstrado na Planilha de controle da respectiva Ata e corroborada pela informação **DMSU e ASDIADM**, (eventos 4307247, 4307403 e 4331771), respectivamente.

À SPADG para a expedição de Ofício ao interessado, acompanhado dos documentos indicados no evento 4331771.

Documento assinado eletronicamente por **Jonas Demostene Ramos**, **Diretor Geral**, em 19/05/2022, às 15:39, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **4336702** e o código CRC **0407E207**.

PODER JUDICIÁRIO

TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS

Palácio da Justiça Rio Tocantins, Praça dos Girassóis, sn - Bairro Centro - CEP 77015007 - Palmas - TO - http://www.tjto.jus.br

PROCESSO	22.0.000011991-5
INTERESSADO	Luiz Carlos Bastos Prata - Secretário Municipal de Administração, Anderson Ramos dos Santos - Diretor de Tecnologia da Informação, Prefeitura Municipal de Alagoinhas - Bahia, Desembargador João Rigo Guimarães - Presidente do Tribunal de Justiça do Estado do Tocantins
ASSUNTO	Pedido de adesão - ARP

Despacho Nº 31114 / 2022 - PRESIDÊNCIA/DIGER/DTINF/DMSU

Em atenção ao **Despacho Nº 30689/2022 - PRESIDÊNCIA/DIGER/DTINF/GABDTI,** evento 4304751, manifesto favoravelmente ao pedido da Secretaria Municipal da Administração (SEMAD) - Alagoinhas/BA, Ofício nº 012/2022, sob evento 4292758, referente à adesão da Ata de Registro de Preços nº 93/2021 - Item 2, SEI nº 21.0.000002638-4, resultado do Pregão Eletrônico - SRP nº 39/2021, conforme saldo disponível para adesão demonstrada no documento exarado no evento 4307247.

Ao GABDTI, para conferência e providências de praxe.

Documento assinado eletronicamente por **Danillo Lustosa Wanderley, Chefe de Divisão,** em 04/05/2022, às 15:46, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **4307403** e o código CRC **1592260F.**

Criado por 187237, versão 3 por 187237 em 04/05/2022 15:42:41.

ATA DE REGISTRO DE PREÇOS N° 93/2021 - Pregão Eletrônico - SRP n° 39/2021 (SEI n° 21.0.000002638-4)

Qualitek Tecnologia - Ltda. CNPJ n° 10.224.281/0001-10

ITEM	DESCRIÇÃO	UND. DE MEDIDA	VALOR UNITÁRIO	QUANTITATIVO TOTAL REGISTRADO EM ATA	QUANTIDADE MÁXIMA DE ADESÃO POR ÓRGÃO (50% DO TOTAL)	QUANTIDADE MÁXIMA DE ADESÕES (200% DO TOTAL)	SALDO DISPONÍVEL PARA ADESÃO	CONTRATADO / EMPENHADO TJTO	QUANTIDADE: 1° Pedido de Adesão da Prefeitura Municipal de Taquari/RS, conforme SEI 22.0.000007692-2	QUANTIDADE: 2° Pedido de Adesão da Secretaria Municipal da Administração (SEMAD) - Alagoinhas/BA, conforme SEI 22.0.0000011991-5	QUANTIDADE: 3° Pedido de Adesão do Órgão XXXXXXX, conforme SEI 21.0.000000000	QUANTIDADE: 4° Pedido de Adesão do Órgão XXXXXXX, conforme SEI 21.0.000000000	QUANTIDADE: 5° Pedido de Adesão do Órgão XXXXXXX, conforme SEI 21.0.000000000
2	Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select, com vigência de 36 (trinta e seis) meses.	Unid.	R$ 111,00	650	325	1300	800	SIM	250	250			

PODER JUDICIÁRIO

TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS

Palácio da Justiça Rio Tocantins, Praça dos Girassóis, s/n - Bairro Centro - CEP 77015007 - Palmas - TO - http://www.tjto.jus.br
Tribunal de Justiça

PROCESSO 21.0.000002638-4
INTERESSADO DTINF, DASR, DMSU
ASSUNTO Homologação de procedimento licitatório.

Parecer Nº 923 / 2021 - PRESIDÊNCIA/DIGER/ASJUADMDG

I – RELATÓRIO

Cuidam os presentes de procedimento licitatório de REGISTRO DE PREÇOS, cujo objeto é a renovação e aquisição de licença de solução corporativa de antivírus *Kaspersky Endpoint Security – Versão Business Select*, incluindo atualizações e suporte técnico, pelo período de 36 (trinta e seis) meses, em atendimento às demandas do Poder Judiciário do Estado do Tocantins.

A modalidade licitatória escolhida foi a de Pregão Eletrônico, tipo menor preço por item/grupo, modo de disputa aberto, com ampla concorrência no item 01 e exclusivo para ME/EPP no item 02 (evento 3749152).

Após o trâmite regular dos autos, passando-se pelas fases interna e externa do procedimento licitatório, vê-se que o aviso do certame foi publicado no sistema COMPRASNET e no Diário da Justiça, conforme eventos 3780891 e 3784597.

Conforme a ata da sessão do dia 15/07/2021 não houve a interposição de recurso, razão pela qual os itens 1 e 2 foram adjudicados à empresa QUALITEK TECNOLOGIA LTDA, CNPJ 10.224.281/0001-10, no valor de R$ 377.100,00 (trezentos e setenta e sete mil e cem reais), tudo conforme Mapa de Preços (evento 3690378).

Despacho **COLIC** (evento 3814086), no qual sugere a homologação do certame.

É o relatório.

II – FUNDAMENTAÇÃO

Destaca-se que o presente exame aborda os aspectos jurídicos do processo, como exige a Lei 10.520/2002, o Decreto 8.538/2015, o Decreto Judiciário 136/2014, a Portaria 674/2012, a Instrução Normativa 01/2015, a Lei Complementar 123/2006 e, subsidiariamente, a Lei 8.666/1993, ressaltando-se que a manifestação desta assessoria dar-se-á sob o prisma estritamente jurídico, não abrangendo a conveniência e oportunidade, bem como aspectos de natureza técnica e administrativa.

O pregão eletrônico compreende duas fases distintas, com o planejamento e estudos iniciais e prossegue até a assinatura do respectivo contrato ou emissão do documento correspondente: i) a fase interna ou preparatória que trata dos procedimentos para a abertura do processo de licitação, delimitando e determinando as condições do edital e a fase externa ou executória, a qual inicia-se com a publicação do edital e termina com a contratação do fornecimento do bem ou da prestação do serviço.

Frise-se ser obrigatório constar nos autos o orçamento estimativo elaborado pela Administração para a aferição do valor, conforme estimativa constante na Pesquisa de Mercado e Mapa de Preços, no evento 3735761.

O Pregoeiro utiliza-se do Mapa de Preços em conjunto com o Termo de Referência para a formação do preço de referência, que é utilizado para análise de aceitabilidade das propostas.

Já a fase externa inicia-se com a convocação dos interessados, observando as regras de convocação estabelecidas no artigo 4º, nos incisos I ao VI, da Lei 10.520/02.

Analisando os atos decorrentes das fases da licitação, especificamente a publicação do edital, faz-se necessário mencionar o teor do artigo 4º, inciso V, da Lei 10.520/2002, transcrito abaixo:

> "Artigo 4º A fase externa do pregão será iniciada com a convocação dos interessados e observará as seguintes regras: [...]
>
> V - o prazo fixado para a apresentação das propostas, contado a partir da publicação do aviso, não será inferior a 8 (oito) dias úteis;"

Pelo exposto, considerando-se que a publicação do edital no COMPRASNET ocorreu em 02/07/2021 e a sessão respectiva em 15/07/2021, houve o atendimento ao prazo de oito dias úteis de divulgação, atendendo assim ao princípio da publicidade.

Após a declaração dos vencedores da licitação, inicia-se o prazo para manifestação de intenção de recursos, conforme determina o artigo 4º, inciso XVIII, da Lei 10.520/2002:

> "Artigo 4º. A fase externa do pregão será iniciada com a convocação dos interessados e observará as seguintes regras: [...]
>
> XVIII - declarado o vencedor, qualquer licitante poderá manifestar imediata e motivadamente a intenção de recorrer, quando lhe será concedido o prazo de 3 (três) dias para apresentação das razões do recurso, ficando os demais licitantes desde logo intimados para apresentar contra-razões em igual número de dias, que começarão a correr do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos;"

Note-se ser da competência da Administração, a adjudicação do item para o qual houve a interposição de recurso, com fundamento no artigo 4º, inciso XXI, da Lei 10.520/02:

> "Artigo 4º, XXI - decididos os recursos, a autoridade competente fará a adjudicação do objeto da licitação ao licitante vencedor".
>
> Artigo 27. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto e homologará o procedimento licitatório".

Entretanto, não havendo a manifestação imediata e motivada sobre a intenção em recorrer, ocorrerá a preclusão, exceto se houver questão arguição de nulidade, a qual será reconhecida a qualquer momento. O registro das ocorrências é realizado na Ata da Sessão.

Consigne-se que na ata (evento 3813934) não há qualquer indicativo dos licitantes em recorrer.

III – CONCLUSÃO

Posto isso, ante o preenchimento dos requisitos básicos da licitação escolhida, considerando-se os aspectos de natureza eminentemente técnica e administrativa, esta assessoria manifesta-se pela homologação do Pregão Eletrônico 39/2021 - SRP à empresa QUALITEK TECNOLOGIA

LTDA, CNPJ 10.224.281/0001-10, quanto aos itens 1 e 2, no valor de R$ 377.100,00 (trezentos e setenta e sete mil e cem reais), tudo conforme os itens mencionados Ata da Sessão e Resultado por fornecedor (eventos 3813934 e 3813904).

À consideração superior.

Documento assinado eletronicamente por **Orfila Leite Fernandes, Assessor Jurídico Administrativo da Diretoria-Geral,** em 30/07/2021, às 16:20, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **3830849** e o código CRC **1C35ED73**.

Nota: Outras informações na Comissão de Licitação deste Tribunal, pelo telefone (063)3218-4590, das 12:00 às 18:00 horas, ou pela Internet no site *www.tjto.jus.br.*
Palmas – TO, 27 de agosto de 2021.

Gabriele Batista Crispim
Pregoeira

DIVISÃO DE LICITAÇÃO, CONTRATOS E CONVÊNIOS

Apostilas

EXTRATO DO TERCEIRO TERMO DE APOSTILAMENTO
TERMO DE CREDENCIAMENTO Nº 125/2017
PROCESSO 17.0.000013292-6
CREDENCIANTE: Tribunal de Justiça do Estado do Tocantins
CREDENCIADA: Synelba Rodrigues Brito
OBJETO DO TERMO DE APOSTILAMENTO:
Fica alterado, com fulcro no § 8º do artigo 65 da Lei nº 8.666/93, o Termo de Credenciamento nº 125/2017, firmado entre o Tribunal de Justiça do Estado do Tocantins e Synelba Rodrigues Brito, em virtude da solicitação da Credenciada, evento 3876348, quanto à mudança da cidade que compõem o Núcleo Regional de Atendimento Multidisciplinar de Dianópolis para prestação de serviços na especialidade de serviço social:
De: Núcleo Regional de Atendimento Multidisciplinar de Dianópolis, Comarca de Dianópolis e Cidade de Dianópolis;
Para: Núcleo Regional de Atendimento Multidisciplinar de Dianópolis, Comarca de Dianópolis e Cidade de Rio da Conceição.
O presente Termo de Apostilamento vincula-se, em sua integralidade, ao Termo de Credenciamento nº 125/2017, aos Autos Administrativos 17.0.000013292-6, bem como às disposições da Lei nº. 8.666/93 e suas alterações posteriores, ao Edital de Credenciamento nº 001/2016, republicado por meio do Edital nº 41/2017, no Diário da Justiça nº 3988, de 03 de março de 2017 e, Edital nº 150/2019, Diário da Justiça nº 4505, de 27 de maio de 2019.
DATA DA ASSINATURA: 26 de agosto de 2021.

EXTRATO DO SEGUNDO TERMO DE APOSTILAMENTO
PROCESSO 19.0.000027497-9
CONTRATO Nº. 151/2020
CONTRATANTE: Tribunal de Justiça do Estado do Tocantins
CONTRATADA: Construtora São Miguel Ltda - ME
OBJETO DO TERMO DE APOSTILAMENTO:
presente Instrumento tem por objeto a alteração do item 8.1, da Cláusula Oitava do Contrato nº 151/2020, firmado com a Construtora São Miguel Ltda - ME, conforme Informação nº 27803/2021- DIVPODG, evento 3865145, o qual passará a vigorar com a seguinte redação:
CLÁUSULA OITAVA– DOTAÇÃO ORÇAMENTÁRIA:
8.1. As despesas com a execução do objeto do referido Contrato correrão por conta da Dotação Orçamentária abaixo consignada:
UNIDADE GESTORA: 050100 - Tribunal de Justiça
CLASSIFICAÇÃO ORÇAMENTÁRIA: 05010.02.061.1145.1101
NATUREZA DE DESPESA: 44.90.51
FONTE DE RECURSOS: 0100
e/ou
UNIDADE GESTORA: 060100 - Funjuris
CLASSIFICAÇÃO ORÇAMENTÁRIA: 06010.02.061.1145.3067
NATUREZA DE DESPESA: 44.90.51
FONTE DE RECURSOS: 0240
DATA DA ASSINATURA: 27 de agosto de 2021.

Extratos de contratos

EXTRATO DE CONTRATO
PREGÃO ELETRÔNICO - SRP Nº 39/2021
ATA DE REGISTRO DE PREÇOS Nº 93/2021
PROCESSO 21.0.000020119-4
CONTRATO Nº 218/2021
CONTRATANTE: Tribunal de Justiça do Estado do Tocantins
CONTRATADA: Qualitek Tecnologia - Ltda

OBJETO: renovação e a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – Versão Business Select, incluindo atualizações e suporte técnico, com o objetivo de atender as demandas do Poder Judiciário do Estado do Tocantins.
VALOR: O valor global do presente Instrumento é de R$ 321.600,00 (trezentos e vinte e um mil e seiscentos reais), compreendendo todas as despesas e custos diretos e indiretos necessários à perfeita execução.
VIGÊNCIA: O presente Contrato terá vigência de 36 (trinta e seis) meses, contados a partir do recebimento definitivo da solução adquirida.
DOTAÇÃO ORÇAMENTÁRIA:
UNIDADE GESTORA: 050100 - Tribunal de Justiça
CLASSIFICAÇÃO ORÇAMENTÁRIA: 05010.02.126.1145.2249
NATUREZA DE DESPESA: 33.90.40
FONTE DE RECURSOS: 0100
DATA DA ASSINATURA: 26 de agosto de 2021.

EXTRATO DE CONTRATO
INEXIGIBILIDADE DE LICITAÇÃO
PROCESSO 21.0.000020352-9
CONTRATO Nº 219/2021
CONTRATANTE: Tribunal de Justiça do Estado do Tocantins
CONTRATADA: Paula Pessoa Pereira
OBJETO: Contratação de instrutora para realização do curso Precedentes Judiciais: Teoria e Prática, para servidores e magistrados do Poder Judiciário Tocantinense, na modalidade EaD.
VALOR: O valor do presente Instrumento fica ajustado em R$ 9.000,00 (nove mil reais).
VIGÊNCIA: Este Contrato terá inicio a partir da data de sua assinatura e vigência no seu respectivo crédito orçamentário.
DOTAÇÃO ORÇAMENTÁRIA:
UNIDADE GESTORA: 060100 – Funjuris
CLASSIFICAÇÃO ORÇAMENTÁRIA: 06010.02.128.1145.4180
NATUREZA DE DESPESA: 33.90.36
FONTE DE RECURSOS: 0240
DATA DA ASSINATURA: 26 de agosto de 2021.

Extratos das atas de registro de preços

EXTRATO DA ATA DE REGISTRO DE PREÇOS Nº 74/2021
PROCESSO ADMINISTRATIVO 21.0.000005150-8
PREGÃO ELETRÔNICO – SRP Nº 38/2021
ORGÃO GERENCIADOR: Tribunal de Justiça do Estado do Tocantins
FORNECEDOR REGISTRADO: Comercial Machado - EIRELI
OBJETO: Registro de preços visando à aquisição futura de lixeiras para coleta seletiva para atender as demandas do Poder Judiciário do Estado do Tocantins.
VIGÊNCIA: A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da publicação do extrato no Diário da Justiça Eletrônico - DJE.
DATA DA ASSINATURA: 26 de agosto 2021.

EXTRATO DA ATA DE REGISTRO DE PREÇOS Nº 75/2021
PROCESSO ADMINISTRATIVO 21.0.000005150-8
PREGÃO ELETRÔNICO – SRP Nº 38/2021
ORGÃO GERENCIADOR: Tribunal de Justiça do Estado do Tocantins
FORNECEDOR REGISTRADO: Movimente Brasil - EIRELI
OBJETO: Registro de preços visando à aquisição futura de contêiner de plástico de 500 litros para coleta seletiva para atender as demandas do Poder Judiciário do Estado do Tocantins.
VIGÊNCIA: A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da publicação do extrato no Diário da Justiça Eletrônico - DJE.
DATA DA ASSINATURA: 26 de agosto 2021.

EXTRATO DA ATA DE REGISTRO DE PREÇOS Nº 76/2021
PROCESSO ADMINISTRATIVO 21.0.000005150-8
PREGÃO ELETRÔNICO – SRP Nº 38/2021
ORGÃO GERENCIADOR: Tribunal de Justiça do Estado do Tocantins
FORNECEDOR REGISTRADO: Fortclean Comércio de Equipamentos - EIRELI
OBJETO: Registro de preços visando à aquisição futura de lixeiras para coleta seletiva para atender as demandas do Poder Judiciário do Estado do Tocantins.

PODER JUDICIÁRIO

TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS

Palácio da Justiça Rio Tocantins, Praça dos Girassóis, s/n - Bairro Centro - CEP 77015007 - Palmas - TO - http://www.tjto.jus.br
Tribunal de Justiça

PROCESSO 21.0.000002638-4
INTERESSADO DTINF, DASR, DMSU
ASSUNTO Homologação de procedimento licitatório.

Termo de Homologação Nº 44 / 2021 - PRESIDÊNCIA/DIGER/ASJUADMDG

Cuidam os presentes de procedimento licitatório de REGISTRO DE PREÇOS, cujo objeto é a renovação e aquisição de licença de solução corporativa de antivírus *Kaspersky Endpoint Security – Versão Business Select*, incluindo atualizações e suporte técnico, pelo período de 36 (trinta e seis) meses, em atendimento às demandas do Poder Judiciário do Estado do Tocantins.

Tendo em vista que a licitação foi realizada de acordo com as disposições da legislação de regência, qual seja, a Lei 10.520/2002, os Decretos 5.450/2005 e 8.538/2015, a Lei Complementar 123/2006, o Decreto Judiciário 136/2014 e a Portaria 674/2012 do Poder Judiciário Tocantinense e, subsidiariamente, a Lei 8.666/93, ACOLHO as sugestões propostas pelo Senhor Diretor Geral (evento 3830855) e considerando-se a manifestação da ASJUADMDG (evento 3830849), **HOMOLOGO** o Pregão 39/2021 - SRP à empresa QUALITEK TECNOLOGIA LTDA, CNPJ 10.224.281/0001-10, quanto aos itens 1 e 2, no valor de R$ 377.100,00 (trezentos e setenta e sete mil e cem reais), tudo conforme os itens mencionados Ata da Sessão e Resultado por fornecedor (eventos 3813934 e 3813904).

Encaminhem-se os autos sucessivamente à:

1. ASPRE para homologação perante o sistema COMPRASNET, extração de cópia do respectivo ato e juntada ao presente feito, bem assim, publicação do presente Termo de Homologação e anexado ao SEI; e

2. DCC para as medidas referentes à formalização da ata de registro de preços/instrumento contratual e;

3. DIFIN para emissão da respectiva Nota de Empenho.

Concomitante, à **DMSU/DTINF** para ciência e acompanhamento.

Cumpra-se.

---

sei! assinatura eletrônica

Documento assinado eletronicamente por **Desembargador João Rigo Guimarães, Presidente,** em 02/08/2021, às 14:19, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **3830858** e o código CRC **40B3978C**.

PODER JUDICIÁRIO

TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS
Palácio da Justiça Rio Tocantins, Praça dos Girassóis, sn - Bairro Centro - CEP 77015007 - Palmas - TO - http://www.tjto.jus.br
Tribunal de Justiça

Contrato Nº 218/2021 - PRESIDÊNCIA/DIGER/DIADM/DCC

PREGÃO ELETRÔNICO - SRP Nº 39/2021
ATA DE REGISTRO DE PREÇOS 93/2021
PROCESSO ORIGINÁRIO 21.0.000002638-4
PROCESSO 21.0.000020119-4

CONTRATO QUE CELEBRAM ENTRE SI O TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS E A EMPRESA QUALITEK TECNOLOGIA - LTDA.

Pelo presente Instrumento e na melhor forma de direito o **TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS**, inscrito no CNPJ/MF sob o nº 25.053.190/0001-36, com sede na Praça dos Girassóis, s/nº, centro, em Palmas/TO, neste ato representado por o Excelentíssimo Senhor Desembargador **JOÃO RIGO GUIMARÃES**, brasileiro, portador do RG nº 316.531 - SSP/GO, inscrito no CPF/MF sob o nº 056.210.461-53, residente e domiciliado nesta Capital, doravante designado **CONTRATANTE** e, do outro lado, a empresa **QUALITEK TECNOLOGIA - LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 10.224.281/0001-10, com sede à Rua José Ribeiro Dantas, 275, SL 404 e 406, Lagoa Nova, Natal/RN, doravante designada **CONTRATADA**, neste ato representada por seu Sócio-Diretor Comercial, Senhor **DENNIS FERNANDES DE MEDEIROS**, brasileiro, empresário, portador do RG nº 2468043 ITEP/RN, inscrito no CPF/MF sob o nº 084.417.344-45, têm entre si, justo e avençado o presente Contrato, observadas as disposições da Lei nº 10.520/2002 e, subsidiariamente pela Lei 8.666/93, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO:

1.1. O presente Instrumento tem por objeto a renovação e a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – Versão Business Select, incluindo atualizações e suporte técnico, com o objetivo de atender as demandas do Poder Judiciário do Estado do Tocantins, conforme descrição e quantitativos abaixo:

ITEM	DESCRIÇÕES	UND.	QTDE.	VALOR UNITÁRIO	VALOR TOTAL
1	Renovação de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select, com vigência de 36 (trinta e seis) meses.	Und.	2.850	R$ 107,00	R$ 304.950,00
2	Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select, com vigência de 36 (trinta e seis) meses.	Und.	150	R$ 111,00	R$ 16.650,00
Valor total					**R$ 321.600,00**

1.2. A aquisição citada na subcláusula 1.1 obedecerá ao estipulado neste Contrato, bem como as especificações técnicas, forma de execução/entrega e as disposições dos documentos adiante enumerados, constantes do Processo Administrativo do 21.0.000002638-4 e 21.0.000020119-4, do CONTRATANTE, e que, independentemente de transcrição, fazem parte integrante e complementar deste, no que não o contrariarem. São eles:

1.2.1. O Edital do Pregão Eletrônico - SRP nº 39/2021, do CONTRATANTE; e

1.2.2. A Ata de Registro de Preços nº 93/2021, resultado do Pregão Eletrônico – SRP nº 39/2021.

1.2.3. A Proposta de Preços e documentos que o acompanham, firmada pela CONTRATADA em 20 de julho de 2021.

1.3. A aquisição do objeto deste Contrato foi realizada por meio de procedimento licitatório, de acordo com o disposto no art. 1º e parágrafo único e art. 2º parágrafo 1º da Lei nº 10.520/2002, sob a modalidade Pregão, na forma eletrônica, para registro de preços, conforme Edital e Processo Administrativo acima citados.

1.4. A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem, até 25% (vinte e cinco por cento) do valor inicial atualizado deste Contrato.

1.5. Nenhum acréscimo poderá exceder os limites estabelecidos no item anterior, salvo as supressões que poderão exceder os limites legais, quando acordadas entre as Partes.

CLÁUSULA SEGUNDA – DA FORMALIZAÇÃO DO CONTRATO:

2.1. A empresa será convocada para assinatura do instrumento contratual, devendo assiná-lo e restituí-lo no prazo de 5 (cinco) dias corridos, podendo este prazo ser prorrogado, a critério do CONTRATANTE, por igual período e por uma vez, desde que ocorra motivo justificado:

2.1.1. A assinatura deste Contrato será realizada por meio eletrônica, utilizando-se do Sistema Eletrônico de Informações - SEI/TJTO.

2.3. No ato de assinatura deste Contrato, a empresa deverá atender as disposições da Portaria nº 97/2010, quanto à verificação da regularidade fiscal. Se qualquer das certidões apresentadas na fase de habilitação do procedimento licitatório expirar sua validade antes da data de assinatura deste Instrumento ou de seus aditivos, deverá a mesma ser atualizada.

CLÁUSULA TERCEIRA – DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS:

3.1. Renovação de licenças de solução corporativa de antivírus

2.1.1. Características Gerais:

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

3.1.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

3.1.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

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

3.1.2. Servidor de Administração e Console Administrativa

3.1.2.1. Compatibilidade:

3.1.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

3.1.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

3.1.2.1.3. Microsoft Windows Server 2016 x64.

3.1.2.1.4. Microsoft Windows Server 2019 x64.

3.1.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

3.1.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

3.1.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

3.1.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

3.1.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

3.1.2.2. Características:

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

3.1.2.2.2. Console deve ser baseada no modelo cliente/servidor.

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

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

3.1.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

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

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

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

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

3.1.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

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

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

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

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

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

3.1.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

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

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

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

3.1.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

3.1.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

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

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

2.1.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

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

3.1.2.2.25.1. Nome do computador.

3.1.2.2.25.2. Nome do domínio.

3.1.2.2.25.3. Range de IP.

3.1.2.2.25.4. Sistema Operacional.

3.1.2.2.25.5. Máquina virtual.

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

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

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

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

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

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

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

3.1.2.2.33. Deve fornecer as seguintes informações dos computadores:

3.1.2.2.33.1. Se o antivírus está instalado.

3.1.2.2.33.2. Se o antivírus está iniciado.

3.1.2.2.33.3. Se o antivírus está atualizado.

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

3.1.2.2.33.5. Minutos/horas desde a última atualização de vacinas.

3.1.2.2.33.6. Data e horário da última verificação executada na máquina.

3.1.2.2.33.7. Versão do antivírus instalado na máquina.

3.1.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças.

3.1.2.2.33.9. Data e horário de quando a máquina foi ligada.

3.1.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina.

3.1.2.2.33.11. Nome do computador.

3.1.2.2.33.12. Domínio ou grupo de trabalho do computador.

3.1.2.2.33.13. Data e horário da última atualização de vacinas.

3.1.2.2.33.14. Sistema operacional com Service Pack.

3.1.2.2.33.15. Quantidade de processadores.

3.1.2.2.33.16. Quantidade de memória RAM.

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

3.1.2.2.33.18. Endereço IP.

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

3.1.2.2.33.20. Atualizações do Windows Updates instaladas.

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

3.1.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina.

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

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

3.1.2.2.35.1. Alteração de Gateway Padrão.

3.1.2.2.35.2. Alteração de subrede.

3.1.2.2.35.3. Alteração de domínio.

3.1.2.2.35.4. Alteração de servidor DHCP.

3.1.2.2.35.5. Alteração de servidor DNS.

3.1.2.2.35.6. Alteração de servidor WINS.

3.1.2.2.35.7. Alteração de subrede.

3.1.2.2.35.8. Resolução de Nome.

3.1.2.2.35.9. Disponibilidade de endereço de conexão SSL.

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

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

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

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

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

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

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

3.1.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos.

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

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

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

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

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

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

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

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

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

3.1.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

3.1.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

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

3.1.2.2.55.1. Nome do vírus.

3.1.2.2.55.2. Nome do arquivo infectado.

3.1.2.2.55.3. Data e hora da detecção.

3.1.2.2.55.4. Nome da máquina ou endereço IP.

3.1.2.2.55.5. Ação realizada.

3.1.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

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

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

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

3.1.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente.

3.1.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

3.1.3. Estações Windows

3.1.3.1. Compatibilidade:

3.1.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate.

3.1.3.1.2. Microsoft Windows 8 Professional/Enterprise.

3.1.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

3.1.3.1.4. Microsoft Windows 10 Professional/Enterprise.

3.1.3.2. Características:

3.1.3.2.1. Deve prover as seguintes proteções:

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

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

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

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

3.1.3.2.1.5. Firewall com IDS.

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

3.1.3.2.1.7. Controle de dispositivos externos.

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

3.1.3.2.1.9. Controle de acesso a sites por horário.

3.1.3.2.1.10. Controle de acesso a sites por usuários.

3.1.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

3.1.3.2.1.12. Controle de execução de aplicativos.

3.1.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

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

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

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

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

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

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

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

3.1.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

3.1.3.2.12. Capacidade de verificar objetos usando heurística.

3.1.3.2.13. Capacidade de agendar uma pausa na verificação.

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

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

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

3.1.3.2.16.1. Perguntar o que fazer, ou;

3.1.3.2.16.2. Bloquear acesso ao objeto.

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

3.1.3.2.16.2.2. Caso positivo de desinfecção:

3.1.3.2.16.2.2.1. Restaurar o objeto para uso.

3.1.3.2.16.2.3. Caso negativo de desinfecção:

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

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

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

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

3.1.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

3.1.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

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

3.1.3.2.22.1. Perguntar o que fazer, ou;

3.1.3.2.22.2. Bloquear o e-mail.

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

3.1.3.2.22.2.2. Caso positivo de desinfecção:

3.1.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

3.1.3.2.22.2.3. Caso negativo de desinfecção:

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

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

3.1.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

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

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

3.1.3.2.27. Deve ter suporte total ao protocolo Ipv6.

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

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

3.1.3.2.29.1. Perguntar o que fazer, ou;

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

3.1.3.2.29.3. Permitir acesso ao objeto.

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

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

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

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

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

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

3.1.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

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

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

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

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

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

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

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

3.1.3.2.39.1. Discos de armazenamento locais.

3.1.3.2.39.2. Armazenamento removível.

3.1.3.2.39.3. Impressoras.

3.1.3.2.39.4. CD/DVD.

3.1.3.2.39.5. Drives de disquete.

3.1.3.2.39.6. Modems.

3.1.3.2.39.7. Dispositivos de fita.

3.1.3.2.39.8. Dispositivos multifuncionais.

3.1.3.2.39.9. Leitores de smart card.

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

3.1.3.2.39.11. Wi-Fi.

3.1.3.2.39.12. Adaptadores de rede externos.

3.1.3.2.39.13. Dispositivos MP3 ou smartphones.

3.1.3.2.39.14. Dispositivos Bluetooth.

3.1.3.2.39.15. Câmeras e Scanners.

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

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

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

3.1.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

3.1.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

3.1.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

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

3.1.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

3.1.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

3.1.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

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

3.1.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

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

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

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

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

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

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

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

3.1.4. Estações Mac OS X

3.1.4.1. Compatibilidade:

3.1.4.1.1. OS X 10.9 (Mavericks).

3.1.4.1.2. OS X 10.10 (Yosemite).

3.1.4.1.3. OS X 10.11 (El Capitan).

3.1.4.1.4. macOS 10.12 (Sierra).

3.1.4.1.5. macOS 10.13 (High Sierra).

3.1.4.1.6. macOS 10.14 (Mojave).

3.1.4.1.7. macOS 10.15 (Catalina).

3.1.4.1.8. macOS 11.0 (Big Sur).

3.1.4.2. Características:

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

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

3.1.4.2.3. Possuir módulo de bloqueio a ataques na rede.

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

3.1.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

3.1.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

3.1.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

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

3.1.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

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

3.1.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

3.1.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

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

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

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

3.1.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

3.1.4.2.17. Capacidade de verificar objetos usando heurística.

3.1.4.2.18. Capacidade de agendar uma pausa na verificação.

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

3.1.4.2.19.1. Perguntar o que fazer, ou;

3.1.4.2.19.2. Bloquear acesso ao objeto.

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

3.1.4.2.19.3.1. Caso positivo de desinfecção:

3.1.4.2.19.3.1.1. Restaurar o objeto para uso.

3.1.4.2.19.3.2. Caso negativo de desinfecção:

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

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

3.1.4.2.21. Capacidade de verificar arquivos de formato de email.

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

3.1.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

3.1.5. Estações Linux

3.1.5.1. Compatibilidade:

3.1.5.1.1. Plataforma 32 bits:

3.1.5.1.1.1. Ubuntu 16.04 LTS

3.1.5.1.1.2. Red Hat® Enterprise Linux® 6.7

3.1.5.1.1.3. CentOS-6.7

3.1.5.1.1.4. Debian GNU / Linux 9.4

3.1.5.1.2. Plataforma 64 bits:

3.1.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

3.1.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

3.1.5.1.2.3. CentOS-6.7, 7.2, 8.0

3.1.5.1.2.4. Debian GNU / Linux 9.4, 10.1

3.1.5.1.2.5. OracleLinux 7.3, 8

3.1.5.1.2.6. SUSE® Linux Enterprise Server 15

3.1.5.1.2.7. openSUSE® 15

3.1.5.1.2.8. Amazon Linux AMI

3.1.5.2. Características:

3.1.5.2.1. Deve prover as seguintes proteções:

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

3.1.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

3.1.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

3.1.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

3.1.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

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

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

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

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

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

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

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

3.1.5.2.13.1. Alta.

3.1.5.2.13.2. Média.

3.1.5.2.13.3. Baixa.

3.1.5.2.13.4. Recomendado.

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

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

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

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

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

3.1.5.2.19. Capacidade de verificar objetos usando heurística.

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

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

3.1.6. Servidores Windows

3.1.6.1. Compatibilidade:

3.1.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

3.1.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

3.1.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

3.1.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

3.1.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

3.1.6.1.6. Microsoft Windows Server 2016.

3.1.6.1.7. Microsoft Windows Server 2019.

3.1.6.2. Características:

3.1.6.2.1. Deve prover as seguintes proteções:

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

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

3.1.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

3.1.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

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

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

3.1.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

3.1.6.2.4.3. Leitura de configurações.

3.1.6.2.4.4. Modificação de configurações.

3.1.6.2.4.5. Gerenciamento de Backup e Quarentena.

3.1.6.2.4.6. Visualização de relatórios.

3.1.6.2.4.7. Gerenciamento de relatórios.

3.1.6.2.4.8. Gerenciamento de chaves de licença.

3.1.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

3.1.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

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

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

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

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

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

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

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

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

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

escolhido seja ignorado.

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

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

3.1.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

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

3.1.6.2.19. Capacidade de verificar objetos usando heurística.

3.1.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

3.1.6.2.21. Capacidade de agendar uma pausa na verificação.

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

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

3.1.6.2.23.1. Perguntar o que fazer, ou;

3.1.6.2.23.2. Bloquear acesso ao objeto.

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

3.1.6.2.23.2.2. Caso positivo de desinfecção:

3.1.6.2.23.2.2.1. Restaurar o objeto para uso.

3.1.6.2.23.3. Caso negativo de desinfecção:

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

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

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

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

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

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

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

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

3.1.7. Servidores Linux

3.1.7.1. Compatibilidade:

3.1.7.1.1. Plataforma 32 bits:

3.1.7.1.1.1. Ubuntu 16.04 LTS.

3.1.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

3.1.7.1.1.3. CentOS-6.7.

3.1.7.1.1.4. Debian GNU / Linux 9.4.

3.1.7.1.2. Plataforma 64 bits:

3.1.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

3.1.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

3.1.7.1.2.3. CentOS-6.7, 7.2, 8.0.

3.1.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

3.1.7.1.2.5. OracleLinux 7.3, 8.

3.1.7.1.2.6. SUSE® Linux Enterprise Server 15.

3.1.7.1.2.7. openSUSE® 15.

3.1.7.1.2.8. Amazon Linux AMI.

3.1.7.2. Características:

3.1.7.2.1. Deve prover as seguintes proteções:

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

3.1.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

3.1.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

3.1.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

2.1.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

3.1.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

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

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

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

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

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

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

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

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

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

3.1.7.2.7. Capacidade de verificar objetos usando heurística.

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

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

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

3.1.8. Smartphones e tablets

3.1.8.1. Compatibilidade:

3.1.8.1.1. Dispositivos com os sistemas operacionais:

3.1.8.1.1.1. Android 4.2 – 11.

3.1.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

3.1.8.2. Características:

3.1.8.2.1. Deve prover as seguintes proteções:

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

3.1.8.2.1.2. Proteção contra adware e autodialers.

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

3.1.8.2.1.4. Arquivos abertos no smartphone.

3.1.8.2.1.5. Programas instalados usando a interface do smartphone

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

3.1.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

3.1.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

3.1.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

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

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

3.1.8.2.7. Deverá ter firewall pessoal (Android).

3.1.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

3.1.8.2.9. Capacidade de enviar comandos remotamente de:

3.1.8.2.9.1. Localizar.

3.1.8.2.9.2. Bloquear.

3.1.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

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

3.1.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

3.1.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

3.1.8.2.14. Capacidade de localizar o dispositivo quando necessário.

3.1.8.2.15. Permitir atualização das definições quando estiver em "roaming".

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

3.1.8.2.17. Deve permitir verificar somente arquivos executáveis.

3.1.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

3.1.8.2.19. Capacidade de agendar uma verificação.

3.1.8.2.20. Capacidade de enviar URL de instalação por e-mail.

3.1.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

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

3.1.8.2.22.1. Deletar.

3.1.8.2.22.2. Ignorar.

3.1.8.2.22.3. Quarentenar.

3.1.8.2.22.4. Perguntar ao usuário.

3.1.9. Gerenciamento de dispositivos móveis (MDM):

3.1.9.1. Compatibilidade:

3.1.9.1.1. Android 4.2 – 11.

3.1.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

3.1.9.2. Características:

3.1.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

3.1.9.2.2. Capacidade de ajustar as configurações de:

3.1.9.2.2.1. Sincronização de e-mail.

3.1.9.2.2..2. Uso de aplicativos.

3.1.9.2.2.3. Senha do usuário.

3.1.9.2.2.4. Criptografia de dados.

3.1.9.2.2.5. Conexão de mídia removível.

3.1.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

3.1.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

3.1.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

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

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

3.1.9.2.8. Permitir sincronização com perfil do "Touch Down".

3.1.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

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

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

3.2. Aquisição de licenças de solução corporativa de antivírus

3.2.1. Características Gerais

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

3.2.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

3.2.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

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

3.2.2. Servidor de Administração e Console Administrativa

3.2.2.1. Compatibilidade:

3.2.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

3.2.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

3.2.2.1.3. Microsoft Windows Server 2016 x64.

3.2.2.1.4. Microsoft Windows Server 2019 x64.

3.2.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

3.2.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

3.2.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

3.2.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

3.2.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

3.2.2.2. Características:

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

3.2.2.2.2. Console deve ser baseada no modelo cliente/servidor.

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

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

3.2.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

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

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

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

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

3.2.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

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

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

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

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

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

3.2.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

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

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

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

3.2.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

3.2.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

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

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

3.2.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

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

3.2.2.2.25.1. Nome do computador.

3.2.2.2.25.2. Nome do domínio.

3.2.2.2.25.3. Range de IP.

3.2.2.2.25.4. Sistema Operacional.

3.2.2.2.25.5. Máquina virtual.

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

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

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

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

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

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

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

3.2.2.2.33. Deve fornecer as seguintes informações dos computadores:

3.2.2.2.33.1. Se o antivírus está instalado.

3.2.2.2.33.2. Se o antivírus está iniciado.

3.2.2.2.33.3. Se o antivírus está atualizado.

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

3.2.2.2.33.5. Minutos/horas desde a última atualização de vacinas.

3.2.2.2.33.6. Data e horário da última verificação executada na máquina.

3.2.2.2.33.7. Versão do antivírus instalado na máquina.

3.2.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças.

3.2.2.2.33.9. Data e horário de quando a máquina foi ligada.

3.2.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina.

3.2.2.2.33.11. Nome do computador.

3.2.2.2.33.12. Domínio ou grupo de trabalho do computador.

3.2.2.2.33.13. Data e horário da última atualização de vacinas.

3.2.2.2.33.14. Sistema operacional com Service Pack.

3.2.2.2.33.15. Quantidade de processadores.

3.2.2.2.33.16. Quantidade de memória RAM.

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

3.2.2.2.33.18. Endereço IP.

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

3.2.2.2.33.20. Atualizações do Windows Updates instaladas.

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

3.2.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina.

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

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

3.2.2.2.35.1. Alteração de Gateway Padrão.

3.2.2.2.35.2. Alteração de subrede.

3.2.2.2.35.3. Alteração de domínio.

3.2.2.2.35.4. Alteração de servidor DHCP.

3.2.2.2.35.5. Alteração de servidor DNS.

3.2.2.2.35.6. Alteração de servidor WINS.

3.2.2.2.35.7. Alteração de subrede.

3.2.2.2.35.8. Resolução de Nome.

3.2.2.2.35.9. Disponibilidade de endereço de conexão SSL.

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

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

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

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

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

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

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

3.2.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos.

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

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

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

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

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

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

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

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

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

3.2.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

3.2.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

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

3.2.2.2.55.1. Nome do vírus.

3.2.2.2.55.2. Nome do arquivo infectado.

3.2.2.2.55.3. Data e hora da detecção.

3.2.2.2.55.4. Nome da máquina ou endereço IP.

3.2.2.2.55.5. Ação realizada.

3.2.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

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

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

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

3.2.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente.

3.2.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

3.2.3. Estações Windows

3.2.3.1. Compatibilidade:

3.2.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate.

3.2.3.1.2. Microsoft Windows 8 Professional/Enterprise.

3.2.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

3.2.3.1.4. Microsoft Windows 10 Professional/Enterprise.

3.2.3.2. Características:

3.2.3.2.1. Deve prover as seguintes proteções:

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

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

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

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

3.2.3.2.1.5. Firewall com IDS.

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

3.2.3.2.1.7. Controle de dispositivos externos.

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

3.2.3.2.1.9. Controle de acesso a sites por horário.

3.2.3.2.1.10. Controle de acesso a sites por usuários.

3.2.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

3.2.3.2.1.12. Controle de execução de aplicativos.

3.2.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

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

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

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

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

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

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

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

3.2.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

3.2.3.2.12. Capacidade de verificar objetos usando heurística.

3.2.3.2.13. Capacidade de agendar uma pausa na verificação.

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

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

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

3.2.3.2.16.1. Perguntar o que fazer, ou;

3.2.3.2.16.2. Bloquear acesso ao objeto.

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

3.2.3.2.16.2.2. Caso positivo de desinfecção:

3.2.3.2.16.2.2.1. Restaurar o objeto para uso.

3.2.3.2.16.2.3. Caso negativo de desinfecção:

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

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

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

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

3.2.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

3.2.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

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

3.2.3.2.22.1. Perguntar o que fazer, ou;

3.2.3.2.22.2. Bloquear o e-mail.

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

3.2.3.2.22.2.2. Caso positivo de desinfecção:

3.2.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

3.2.3.2.22.2.3. Caso negativo de desinfecção:

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

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

3.2.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

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

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

3.2.3.2.27. Deve ter suporte total ao protocolo Ipv6.

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

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

3.2.3.2.29.1. Perguntar o que fazer, ou;

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

3.2.3.2.29.3. Permitir acesso ao objeto.

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

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

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

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

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

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

3.2.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

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

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

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

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

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

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

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

3.2.3.2.39.1. Discos de armazenamento locais.

3.2.3.2.39.2. Armazenamento removível.

3.2.3.2.39.3. Impressoras.

3.2.3.2.39.4. CD/DVD.

3.2.3.2.39.5. Drives de disquete.

3.2.3.2.39.6. Modems.

3.2.3.2.39.7. Dispositivos de fita.

3.2.3.2.39.8. Dispositivos multifuncionais.

3.2.3.2.39.9. Leitores de smart card.

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

3.2.3.2.39.11. Wi-Fi.

3.2.3.2.39.12. Adaptadores de rede externos.

3.2.3.2.39.13. Dispositivos MP3 ou smartphones.

3.2.3.2.39.14. Dispositivos Bluetooth.

3.2.3.2.39.15. Câmeras e Scanners.

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

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

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

3.2.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

3.2.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

3.2.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

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

3.2.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

3.2.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

3.2.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

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

3.2.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

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

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

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

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

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

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

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

3.2.4. Estações Mac OS X

3.2.4.1. Compatibilidade:

3.2.4.1.1. OS X 10.9 (Mavericks).

3.2.4.1.2. OS X 10.10 (Yosemite).

3.2.4.1.3. OS X 10.11 (El Capitan).

3.2.4.1.4. macOS 10.12 (Sierra).

3.2.4.1.5. macOS 10.13 (High Sierra).

3.2.4.1.6. macOS 10.14 (Mojave).

3.2.4.1.7. macOS 10.15 (Catalina).

3.2.4.1.8. macOS 11.0 (Big Sur).

3.2.4.2. Características:

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

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

3.2.4.2.3. Possuir módulo de bloqueio a ataques na rede.

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

3.2.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

3.2.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

3.2.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

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

3.2.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

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

3.2.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

3.2.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

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

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

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

3.2.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

3.2.4.2.17. Capacidade de verificar objetos usando heurística.

3.2.4.2.18. Capacidade de agendar uma pausa na verificação.

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

3.2.4.2.19.1. Perguntar o que fazer, ou;

3.2.4.2.19.2. Bloquear acesso ao objeto.

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

3.2.4.2.19.3.1. Caso positivo de desinfecção:

3.2.4.2.19.3.1.1. Restaurar o objeto para uso.

3.2.4.2.19.3.2. Caso negativo de desinfecção:

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

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

3.2.4.2.21. Capacidade de verificar arquivos de formato de email.

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

3.2.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

3.2.5. Estações Linux

3.2.5.1. Compatibilidade:

3.2.5.1.1. Plataforma 32 bits:

3.2.5.1.1.1. Ubuntu 16.04 LTS

3.2.5.1.1.2. Red Hat® Enterprise Linux® 6.7

3.2.5.1.1.3. CentOS-6.7

3.2.5.1.1.4. Debian GNU / Linux 9.4

3.2.5.1.2. Plataforma 64 bits:

3.2.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

3.2.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

3.2.5.1.2.3. CentOS-6.7, 7.2, 8.0

3.2.5.1.2.4. Debian GNU / Linux 9.4, 10.1

3.2.5.1.2.5. OracleLinux 7.3, 8

3.2.5.1.2.6. SUSE® Linux Enterprise Server 15

3.2.5.1.2.7. openSUSE® 15

3.2.5.1.2.8. Amazon Linux AMI

3.2.5.2. Características

3.2.5.2.1. Deve prover as seguintes proteções:

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

2.2.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

3.2.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

3.2.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

3.2.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

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

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

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

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

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

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

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

3.2.5.2.13.1. Alta.

3.2.5.2.13.2. Média.

3.2.5.2.13.3. Baixa.

3.2.5.2.13.4. Recomendado.

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

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

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

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

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

3.2.5.2.19. Capacidade de verificar objetos usando heurística.

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

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

3.2.6. Servidores Windows

3.2.6.1. Compatibilidade:

3.2.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

3.2.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

3.2.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

3.2.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

3.2.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

3.2.6.1.6. Microsoft Windows Server 2016.

3.2.6.1.7. Microsoft Windows Server 2019.

3.2.6.2. Características:

3.2.6.2.1. Deve prover as seguintes proteções:

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

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

3.2.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

3.2.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

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

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

3.2.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

3.2.6.2.4.3. Leitura de configurações.

3.2.6.2.4.4. Modificação de configurações.

3.2.6.2.4.5. Gerenciamento de Backup e Quarentena.

3.2.6.2.4.6. Visualização de relatórios.

3.2.6.2.4.7. Gerenciamento de relatórios.

3.2.6.2.4.8. Gerenciamento de chaves de licença.

3.2.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

2.2.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

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

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

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

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

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

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

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

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

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

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

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

3.2.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

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

3.2.6.2.19. Capacidade de verificar objetos usando heurística.

3.2.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

3.2.6.2.21. Capacidade de agendar uma pausa na verificação.

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

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

3.2.6.2.23.1. Perguntar o que fazer, ou;

3.2.6.2.23.2. Bloquear acesso ao objeto.

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

3.2.6.2.23.2.2. Caso positivo de desinfecção:

3.2.6.2.23.2.2.1. Restaurar o objeto para uso.

3.2.6.2.23.3. Caso negativo de desinfecção:

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

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

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

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

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

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

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

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

3.2.7. Servidores Linux

3.2.7.1. Compatibilidade:

3.2.7.1.1. Plataforma 32 bits:

3.2.7.1.1.1. Ubuntu 16.04 LTS.

3.2.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

3.2.7.1.1.3. CentOS-6.7.

3.2.7.1.1.4. Debian GNU / Linux 9.4.

3.2.7.1.2. Plataforma 64 bits:

3.2.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

3.2.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

3.2.7.1.2.3. CentOS-6.7, 7.2, 8.0.

3.2.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

3.2.7.1.2.5. OracleLinux 7.3, 8.

3.2.7.1.2.6. SUSE® Linux Enterprise Server 15.

3.2.7.1.2.7. openSUSE® 15.

3.2.7.1.2.8. Amazon Linux AMI.

3.2.7.2. Características:

3.2.7.2.1. Deve prover as seguintes proteções:

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

3.2.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

3.2.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

3.2.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

3.2.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

3.2.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

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

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

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

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

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

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

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

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

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

3.2.7.2.7. Capacidade de verificar objetos usando heurística.

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

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

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

3.2.8. Smartphones e tablets

3.2.8.1. Compatibilidade:

3.2.8.1.1. Dispositivos com os sistemas operacionais:

3.2.8.1.1.1. Android 4.2 – 11.

3.2.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

3.2.8.2. Características:

3.2.8.2.1. Deve prover as seguintes proteções:

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

3.2.8.2.1.2. Proteção contra adware e autodialers.

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

3.2.8.2.1.4. Arquivos abertos no smartphone.

3.2.8.2.1.5. Programas instalados usando a interface do smartphone

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

3.2.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

3.2.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

3.2.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

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

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

3.2.8.2.7. Deverá ter firewall pessoal (Android).

3.2.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

3.2.8.2.9. Capacidade de enviar comandos remotamente de:

3.2.8.2.9.1. Localizar.

3.2.8.2.9.2. Bloquear.

3.2.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

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

3.2.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

3.2.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

3.2.8.2.14. Capacidade de localizar o dispositivo quando necessário.

3.2.8.2.15. Permitir atualização das definições quando estiver em "roaming".

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

3.2.8.2.17. Deve permitir verificar somente arquivos executáveis.

3.2.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

3.2.8.2.19. Capacidade de agendar uma verificação.

3.2.8.2.20. Capacidade de enviar URL de instalação por e-mail.

3.2.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

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

3.2.8.2.22.1. Deletar.

3.2.8.2.22.2. Ignorar.

3.2.8.2.22.3. Quarentenar.

3.2.8.2.22.4. Perguntar ao usuário.

3.2.9. Gerenciamento de dispositivos móveis (MDM):

3.2.9.1. Compatibilidade:

3.2.9.1.1. Android 4.2 – 11.

3.2.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

3.2.9.2. Características:

3.2.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

3.2.9.2.2. Capacidade de ajustar as configurações de:

3.2.9.2.2.1. Sincronização de e-mail.

3.2.9.2.2..2. Uso de aplicativos.

3.2.9.2.2.3. Senha do usuário.

3.2.9.2.2.4. Criptografia de dados.

3.2.9.2.2.5. Conexão de mídia removível.

3.2.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

3.2.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

3.2.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

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

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

3.2.9.2.8. Permitir sincronização com perfil do "Touch Down".

3.2.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

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

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

3.3. Transferência de conhecimento e direitos de propriedade intelectual

3.3.1. O uso de uma solução de antivírus corporativo é imprescindível por conter funções de proteção que vão além de um antivírus comum, evitando, portanto, invasões ou roubos de informações, por exemplo. Por isso, não existe versões corporativas gratuitas, não sendo vislumbrada outra forma de utilização senão a obrigatoriedade da renovação/aquisição dessa tecnologia de terceiros.

3.3.2. Os antivírus corporativos são produtos consolidados no mercado de Tecnologia da Informação e Comunicação no Brasil e utilizados por organizações públicas e privadas. Desta forma, os riscos de descontinuidade desse produto no mercado parecem ser mínimos.

3.3.3. A CONTRATADA deverá realizar a transferência de conhecimento nas versões dos softwares que serão adquiridos pelo Contratante e com isso, repassar informações de configuração, testes, procedimentos de contingência e demais informações necessárias para a operação e manutenção da solução.

3.3.4. Não se aplica o requisito pertinente aos direitos de propriedade intelectual e autoral da STIC, uma vez que não será produzido nenhum artefato, tampouco trata de desenvolvimento de software.

CLÁUSULA QUARTA – DA DINÂMICA DE EXECUÇÃO:

4.1. A tabela abaixo sintetiza as etapas de execução desta contratação. O prazo em todas as etapas tem como referência inicial o fim da etapa anterior.

Etapa	Descrição	Quando ocorre
1	Recebimento do pedido de fornecimento.	O TJTO encaminhará o pedido de fornecimento a qualquer tempo dentro da vigência da Ata de Registro de Preços e após a assinatura do contrato.
2	Entrega das licenças.	O prazo será de até 20 (vinte) dias úteis, contados a partir da data de assinatura do contrato ou recebimento da nota de

		empenho.
3	Recebimento provisório das licenças.	Imediatamente após o recebimento das licenças, para efeito de posterior verificação da conformidade do material com a especificação, nos termos do artigo 73, da Lei nº 8.666, de 1993.
4	Avaliação das licenças entregues.	Após a entrega, será realizada uma avaliação e homologação pelos responsáveis técnicos. A análise para comprovação das características técnicas consistirá em avaliar as documentações apresentadas e também informações de registro das licenças no site oficial do fabricante.
5	Recebimento Definitivo das licenças.	O responsável técnico deverá, após a comprovação do atendimento das especificações técnicas, emitir e assinar em, no máximo, 15 (quinze) dias úteis, contados do primeiro dia útil posterior à entrega dos equipamentos, o Termo de Recebimento Definitivo, nos termos do artigo 73, da Lei nº 8.666, de 1993.
6	Início da contagem do prazo de garantia.	Data da emissão do recebimento definitivo das licenças. Se for o caso de licenças vincendas, a garantia iniciará no dia subsequente após o fim da vigência desta.
7	Fim do prazo de garantia	Após 36 (trinta e seis) meses.

CLÁUSULA QUINTA - DO VALOR:

5.1. O valor global do presente Instrumento é de **R$ 321.600,00 (trezentos e vinte e um mil e seiscentos reais),** compreendendo todas as despesas e custos diretos e indiretos necessários à perfeita execução deste Contrato.

CLÁUSULA SEXTA – DA DOTAÇÃO ORÇAMENTÁRIA:

6.1. A despesa com a execução do objeto deste Contrato correrá à conta da Dotação Orçamentária consignada:

Unidade Gestora: 050100 - Tribunal de Justiça
Classificação Orçamentária: 05010.02.126.1145.2249
Natureza da Despesa: 33.90.40
Fonte do Recurso: 0100

6.2. As despesas inerentes à execução deste Contrato serão liquidadas por meio da Nota de Empenho que será emitida à conta da dotação orçamentária especificada nesta Cláusula.

6.3. **A CONTRATADA emitirá Nota Fiscal em observância à unidade gestora emissora da nota de empenho que albergou a aquisição.**

CLÁUSULA SÉTIMA – DO PAGAMENTO:

7.1. A CONTRATADA deverá, obrigatoriamente, apresentar nota fiscal correspondente aos objetos fornecidos.

7.2. Os pagamentos serão efetuados após análise da conformidade dos objetos entregues discriminado na respectiva nota fiscal e o atesto do gestor do contrato.

7.3. O atesto do gestor do contrato na nota fiscal é condição indispensável para o pagamento:

7.3.1. Na ausência do gestor do contrato (férias, licença ou em viagem por interesse do CONTRATANTE), o atesto será dado pelo gestor substituto.

7.4. O CONTRATANTE reserva-se o direito de não atestar a nota fiscal para o pagamento, se os dados constantes desta estiverem em desacordo com os dados da CONTRATADA ou, ainda, se os objetos fornecidos não estiverem em conformidade com as especificações apresentadas neste Instrumento e no Termo de Referência, ficando o pagamento suspenso até a regularização.

7.5. O pagamento será efetuado em até 30 (trinta) dias corridos, após o protocolo de recebimento da nota fiscal (momento em que o credor está adimplente com a obrigação firmada perante o CONTRATANTE), sendo que, recaindo sobre dias não úteis, o termo final será prorrogado para o dia útil subsequente.

7.6. O pagamento será realizado, no prazo previsto no item anterior, por meio de ordem bancária em conta corrente da CONTRATADA: **Banco Caixa Econômica Federal - 104, Agência nº 1585 / Operação 003, Conta Corrente 2852-4**, quando mantidas as mesmas condições iniciais de habilitação e caso não haja fato impeditivo para o qual não tenha concorrido.

7.7. O CNPJ constante da Nota Fiscal deverá ser o mesmo indicado na proposta e nota de empenho e vinculado à conta-corrente.

7.8. O CONTRATANTE somente pagará à CONTRATADA o que for solicitado e entregue.

7.9. Ocorrendo atraso no pagamento, e desde que tal não tenha concorrido de alguma forma à CONTRATADA, haverá incidência de atualização monetária sobre o valor devido, pela variação acumulada do índice Geral de Preços – Disponibilidade Interna (IGP-DI), coluna 2, publicado pela FGV, ocorrida entre a data final prevista para o pagamento e a data de sua efetiva realização.

7.10. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

7.11. Todos os atos inerentes ao presente processo obedecerão às regras concernentes ao Sistema Eletrônico de Informações – SEI do CONTRATANTE.

CLÁUSULA OITAVA – DO REAJUSTE E ALTERAÇÕES:

8.1. O valor contratado é fixo e irreajustável.

8.2. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA:

9.1. A CONTRATADA obriga-se a:

9.1.1. Observar as leis, decretos, regulamentos, portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto deste Contrato;

9.1.2. Cumprir todas as obrigações constantes neste Instrumento, no Edital, seus Anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução deste Contrato;

9.1.3. Atender prontamente às solicitações do CONTRATANTE no fornecimento do objeto nas quantidades e especificações deste Termo de Referência, de acordo com a necessidade desta Corte, a partir da solicitação do gestor do contrato.

9.1.4. Responsabilizar-se por todos os recursos e insumos necessários ao perfeito cumprimento do objeto contratado, devendo estar incluídas no preço proposto todas as despesas com materiais, insumos, seguros, impostos, taxas, encargos e demais despesas necessárias à perfeita execução do objeto.

9.1.5. Indicar, formalmente, preposto apto a representá-la junto ao CONTRATANTE, que deverá responder pela fiel execução do contrato.

9.1.6. Prestar todos os esclarecimentos técnicos que lhe forem solicitados pelo Contratante, relacionados com as características e funcionamento do objeto, inclusive em relação aos problemas detectados.

9.1.7. Comunicar, imediatamente, por escrito qualquer anormalidade, prestando ao Contratante os esclarecimentos julgados necessários.

9.1.8. Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados; treinados e qualificados para prestação dos serviços.

9.1.9. Manter ficha de controle do serviço, na qual serão relatadas todas as ocorrências.

9.1.10. Assumir inteira responsabilidade técnica e operacional, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas na prestação do objeto.

9.1.11. Ficar obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nas aquisições até 25% (vinte e cinco por cento) do valor inicial deste Termo de Referência, nos termos da Lei.

9.1.12. Não transferir a outrem, no todo ou em parte, o objeto desta prestação.

9.1.13. Identificar qualquer equipamento de sua posse que venha a ser utilizado nas dependências do CONTRATANTE, afixando placas de controle patrimonial, selos de segurança etc.

9.1.14. Reparar quaisquer danos diretamente causados ao CONTRATANTE ou a terceiros, por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da presente relação contratual, não excluindo ou reduzindo essa responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pelo Contratante.

9.1.15. Cumprir integralmente as exigências do Acordo de Nível de Serviço, disposto no "ANEXO C" do Termo de Referência.

9.1.16. Manter sigilo sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa.

9.1.17. Manter, durante a execução deste Contrato, todas as condições de habilitação e qualificação exigidas na licitação, em conformidade com art. 55, inciso XIII, da Lei nº 8.666/93, incluindo a atualização de documentos de controle da arrecadação de tributos e contribuições federais e outras legalmente exigíveis.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DO CONTRATANTE:

10.1. O CONTRATANTE obriga-se a:

10.1.1. Observar as leis, decretos, regulamentos, portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto deste Contrato;

10.1.2. Responsabilizar-se pela lavratura do respectivo contrato ou instrumento equivalente, com base nas disposições da Lei n°. 8.666/93 e suas alterações;

10.1.3. Receber os objetos de acordo com as disposições deste Contrato e do Termo de Referência;

10.1.4. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

10.1.5. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

10.1.6. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, por meio de comissão/servidor especialmente designado;

10.1.8. Prestar quaisquer esclarecimentos que venham ser formalmente solicitados pelo FORNECEDOR e pertinente ao objeto desta Ata;

10.1.9. Zelar pelo bom andamento da presente aquisição/contratação, dirimindo quaisquer dúvidas que porventura existam;

10.1.10. Assegurar os recursos orçamentários e financeiros para custear a execução deste Contrato.

10.1.11. Processar e liquidar a fatura correspondente, por meio de Ordem Bancária, desde que não haja fato impeditivo imputado à CONTRATADA;

10.1.12. Zelar para que durante a vigência deste Contrato sejam cumpridas as obrigações assumidas por parte da CONTRATADA, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas.

CLÁUSULA DÉCIMA PRIMEIRA – SANÇÕES ADMINISTRATIVAS:

11.1. A CONTRATADA que, convocada dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar a documentação exigida ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedida de licitar e contratar com a Administração Pública do Estado do Tocantins e será descredenciada no Sistema de Cadastramento Unificado de Fornecedores (Sicaf), pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais;

11.2. Subsidiariamente, nos termos do art. 87 da Lei n°. 8.666/93, pela inexecução total ou parcial das condições estabelecidas neste Instrumento, o CONTRATANTE poderá, garantida a prévia defesa da CONTRATADA, que deverá ser apresentada no prazo de 5 (cinco) dias úteis a contar da sua notificação, aplicar, sem prejuízo das responsabilidades penal e civil, as seguintes sanções:

a) Advertência, por escrito, quando a CONTRATADA deixar de atender quaisquer indicações aqui constantes;

b) Multa compensatória/indenizatória no percentual de 5% (cinco por cento) calculado sobre o valor contratado;

c) Suspensão temporária de participação em licitação e impedimento de contratar com o Poder Judiciário do Estado do Tocantins, pelo prazo de até 2 (dois) anos; e

d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATAD A ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

11.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pela CONTRATADA, a esta será aplicada multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor deste Contrato, por dia de atraso, limitada a 10% (dez por cento) do valor inadimplido;

11.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhido ao Fundo Especial de Modernização e Aprimoramento do Poder Judiciário - Funjuris, dentro do prazo de 5 (cinco) dias úteis após a respectiva notificação;

11.5. Caso não seja paga no prazo previsto no subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado pelo Poder Judiciário do Estado do Tocantins ou cobrada judicialmente;

11.6. Além das penalidades citadas, a CONTRATADA ficará sujeita, ainda, no que couber, às demais penalidades referidas no Capítulo IV da Lei nº. 8.666/93.

CLÁUSULA DÉCIMA SEGUNDA – DA RESCISÃO:

12.1. O presente Instrumento poderá ser rescindido:

a) Por ato unilateral e escrito da Administração, nos casos enumerados nos incisos I a XII e XVII e XVIII do art. 78, da Lei 8.666/93;

b) Amigavelmente, por acordo entre as partes, reduzido a termo no respectivo procedimento administrativo, desde que haja conveniência para a Administração; ou

c) Judicialmente, nos termos da Lei.

Parágrafo Único – No caso de rescisão amigável, a parte que pretender rescindir o Contrato comunicará sua intenção à outra, por escrito.

12.2. A CONTRATADA reconhece os direitos do CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993:

12.2.1. A inexecução total ou parcial deste Contrato ensejará a sua rescisão, com às consequências estabelecidas neste Instrumento e as previstas em lei.

CLÁUSULA DÉCIMA TERCEIRA – DA VINCULAÇÃO:

13.1. O presente Contrato fica vinculado aos autos 21.0.000002638-4 e 21.0.000020119-4.

CLÁUSULA DÉCIMA QUARTA – DA LEGISLAÇÃO E CASOS OMISSOS:

14.1. O presente Instrumento, inclusive os casos omissos, regula-se pela Lei nº 10.520/2002, pelo Decreto nº 10.024/2019 e, subsidiariamente, pela Lei nº 8.666/1993 e suas alterações posteriores.

CLÁUSULA DÉCIMA QUINTA – DA VIGÊNCIA:

15.1. O presente Contrato terá vigência de 36 (trinta e seis) meses, contados a partir do recebimento definitivo da solução adquirida.

CLÁUSULA DÉCIMA SEXTA – DAS VEDAÇÕES:

16.1. É vedado à CONTRATADA:

16.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

16.1.2. Subcontratar, no todo ou em parte, a execução do objeto deste Contrato, sem anuência do CONTRATANTE;

16.1.3. Interromper a execução contratual sob alegação de inadimplemento por parte do CONTRATANTE, salvo nos casos previstos em lei.

CLÁUSULA DÉCIMA SÉTIMA – DA PUBLICAÇÃO:

17.1. A publicação resumida do presente Contrato no Diário da Justiça - DJE, que é condição indispensável para sua eficácia, será providenciada pelo CONTRATANTE, nos termos do parágrafo único do artigo 61 de Lei nº 8.666/93.

CLÁUSULA DÉCIMA OITAVA – DA GESTÃO E FISCALIZAÇÃO:

18.1. Profissionais da CONTRATADA: equipe composta por técnicos da CONTRATADA, responsáveis pela execução e acompanhamento do objeto.

18.1.1. Técnico: funcionário da CONTRATADA, responsável pela execução técnica-operacional.

18.1.2. Preposto: funcionário representante da CONTRATADA, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

18.2. Equipe de Gestão do Contrato: equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares.

18.2.1. Gestor do Contrato: servidor responsável pela gestão contratual, conforme Decreto Judiciário nº 291, de 2009 e Portaria nº 255, de 2009, do Tribunal de Justiça do Estado do Tocantins.

18.2.2. Fiscal Demandante: servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos funcionais da solução.

18.2.3. Fiscal Técnico: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.

18.2.4. Fiscal Administrativo: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

18.3. A atuação ou a eventual omissão da Fiscalização durante a realização dos trabalhos, não poderá ser invocada para eximir a CONTRATADA da responsabilidade no fornecimento dos produtos.

18.4. A fiscalização será sob o aspecto qualitativo e quantitativo, devendo ser anotado, em registro próprio as falhas detectadas, e comunicadas ao gestor do contrato todas as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte da CONTRATADA.

18.5. A comunicação entre a fiscalização e a CONTRATADA será realizada por meio de correspondência oficial e anotações ou registros no mesmo processo que tratam da aquisição dos objetos.

18.6. Quando houver necessidade o gestor deverá emitir notificações para a CONTRATADA.

CLÁUSULA DÉCIMA NONA – DAS CONDIÇÕES GERAIS:

19.1. O CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA de seus empregados, prepostos ou subordinados.

CLÁUSULA VIGÉSIMA – DO FORO:

20.1. Para dirimir todas as questões oriundas da execução do presente Contrato fica eleito o Foro de Palmas - TO, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

E, para firmeza e como prova de assim haverem, entre si, ajustado e contratado, firmam este Contrato, para que surta seus efeitos legais, por meio de assinatura eletrônica, utilizando-se do Sistema Eletrônico de Informações - SEI.

Documento assinado eletronicamente por **Dennis Fernandes de Medeiros**, **Usuário Externo**, em 26/08/2021, às 09:17, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Desembargador João Rigo Guimarães**, **Presidente**, em 26/08/2021, às 17:21, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **3876515** e o código CRC **064DF768**.

925814.392021 .5695 .4551 .419100

Tribunal de Justiça do Estado de Tocantins

Ata de Realização do Pregão Eletrônico
Nº 00039/2021 (SRP)

Às 14:00 horas do dia 15 de julho de 2021, reuniram-se o Pregoeiro Oficial deste Órgão e respectivos membros da Equipe de Apoio, designados pelo instrumento legal Portaria n.º 145/2021 de 26/01/2021, em atendimento às disposições contidas na Lei nº 10.520 de 17 de julho de 2002 e no Decreto nº 10.024 de 20 de setembro de 2019, referente ao Processo nº 21.0.000002638-4, para realizar os procedimentos relativos ao Pregão nº 00039/2021. Modo de disputa: Aberto. Objeto: Contratação de empresa especializada objetivando a renovação e a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – Versão Business Select, incluindo atualizações e suporte técnico, para atender as demandas do Poder Judiciário do Estado do Tocantins.. O Pregoeiro abriu a Sessão Pública em atendimento às disposições contidas no edital, divulgando as propostas recebidas. Abriu-se em seguida a fase de lances para classificação dos licitantes relativamente aos lances ofertados.

Item: 1
Descrição: "software"
Descrição Complementar: "software", aplicação: informática, tipo: client server suite, características adicionais: antivírus corporativo, atualização contínua e su-
Tratamento Diferenciado: -
Quantidade: 2.850
Valor Estimado: R$ 113,1900
Aplicabilidade Decreto 7174: Não
Intervalo mínimo entre lances: 1,00 %
Unidade de fornecimento: Unidade
Situação: Aceito e Habilitado
Aplicabilidade Margem de Preferência: Não

Aceito para: QUALITEK TECNOLOGIA LTDA**, pelo melhor lance de** R$ 108,0000 **e com valor negociado a** R$ 107,0000 **e a quantidade de** 2.850 **Unidade** .

Item: 2
Descrição: "software"
Descrição Complementar: "software", aplicação: informática, tipo: client server suite, características adicionais: antivírus corporativo, atualização contínua e su-
Tratamento Diferenciado: Tipo I - Participação Exclusiva de ME/EPP/Equiparada
Quantidade: 650
Valor Estimado: R$ 117,2000
Aplicabilidade Decreto 7174: Não
Intervalo mínimo entre lances: 1,00 %
Unidade de fornecimento: Unidade
Situação: Aceito e Habilitado
Aplicabilidade Margem de Preferência: Não

Aceito para: QUALITEK TECNOLOGIA LTDA**, pelo melhor lance de** R$ 112,0000 **e com valor negociado a** R$ 111,0000 **e a quantidade de** 650 **Unidade** .

Histórico

Item: 1 - "software"

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.
(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	ME/EPP	Declaração	Quantidade	Valor Unit.	Valor Global	Data/Hora

		Equiparada	ME/EPP				Registro
10.224.281/0001-10	QUALITEK TECNOLOGIA LTDA	Sim	Sim	2.850	R$ 110,0000	R$ 313.500,0000	14/07/2021 18:27:05

Marca: Kaspersky
Fabricante: Kaspersky
Modelo / Versão: Endpoint Security for Business Select 36 meses
Descrição Detalhada do Objeto Ofertado: Renovação de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select, com vigência de 36 meses.
Porte da empresa: ME/EPP

19.585.941/0001-62	SATURNO SOFTWARE E SISTEMAS LTDA	Sim	Sim	2.850	R$ 113,1900	R$ 322.591,5000	14/07/2021 15:47:40

Marca: Kaspersky
Fabricante: Kaspersky
Modelo / Versão: Business Select
Descrição Detalhada do Objeto Ofertado: Renovação de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select.
Porte da empresa: ME/EPP

13.497.079/0001-50	ALLSEC SERVICOS EM TECNOLOGIA DA INFORMACAO LTDA	Sim	Sim	2.850	R$ 113,1900	R$ 322.591,5000	15/07/2021 10:06:41

Marca: KASPERSKY
Fabricante: KASPERSKY LAB
Modelo / Versão: Kaspersky Endpoint Security –Versão Business Selec
Descrição Detalhada do Objeto Ofertado: Renovação de licenças do software de antivírus Kaspersky Endpoint Security –Versão Business Select.
Porte da empresa: ME/EPP

35.840.944/0001-51	LAZZACLEAN SERVICOS DE PORTARIAS LTDA	Sim	Sim	2.850	R$ 299,0000	R$ 852.150,0000	15/07/2021 11:55:53

Marca: KASPERSKY
Fabricante: KASPERSKY
Modelo / Versão: ENDPOINT
Descrição Detalhada do Objeto Ofertado: Renovação de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select.
Porte da empresa: ME/EPP

Lances (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R$ 299,0000	35.840.944/0001-51	15/07/2021 14:00:00:450
R$ 113,1900	13.497.079/0001-50	15/07/2021 14:00:00:450
R$ 113,1900	19.585.941/0001-62	15/07/2021 14:00:00:450
R$ 110,0000	10.224.281/0001-10	15/07/2021 14:00:00:450
R$ 108,0000	10.224.281/0001-10	15/07/2021 14:08:47:937

Não existem lances de desempate ME/EPP para o item

Eventos do Item

Evento	Data	Observações
Abertura	15/07/2021 14:00:01	Item aberto.
Encerramento etapa aberta	15/07/2021 14:10:48	Encerrada etapa aberta do item.
Sorteio eletrônico	15/07/2021 14:10:48	Item teve empate real para o valor 113,1900. Procedeu-se o sorteio eletrônico entre os fornecedores com propostas empatadas.

Encerramento	15/07/2021 14:10:48	Item encerrado.
Abertura do prazo - Convocação anexo	20/07/2021 13:44:42	Convocado para envio de anexo o fornecedor QUALITEK TECNOLOGIA LTDA, CNPJ/CPF: 10.224.281/0001-10.
Encerramento do prazo - Convocação anexo	20/07/2021 13:56:47	Encerrado o prazo de Convocação de Anexo pelo fornecedor QUALITEK TECNOLOGIA LTDA, CNPJ/CPF: 10.224.281/0001-10.
Aceite de proposta	20/07/2021 14:05:37	Aceite individual da proposta. Fornecedor: QUALITEK TECNOLOGIA LTDA, CNPJ/CPF: 10.224.281/0001-10, pelo melhor lance de R$ 108,0000 e com valor negociado a R$ 107,0000. Motivo: Proposta Negociada via chat
Habilitação de fornecedor	20/07/2021 14:07:25	Habilitação em grupo de propostas. Fornecedor: QUALITEK TECNOLOGIA LTDA - CNPJ/CPF: 10.224.281/0001-10

Não existem intenções de recurso para o item

Item: 2 - "software"

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.
(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	ME/EPP Equiparada	Declaração ME/EPP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
10.224.281/0001-10	QUALITEK TECNOLOGIA LTDA	Sim	Sim	650	R$ 115,0000	R$ 74.750,0000	14/07/2021 18:27:05
	Marca: Kaspersky **Fabricante:** Kaspersky **Modelo / Versão:** Endpoint Security for Business Select 36 meses **Descrição Detalhada do Objeto Ofertado:** Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select, com vigência de 36 meses. **Porte da empresa:** ME/EPP						
19.585.941/0001-62	SATURNO SOFTWARE E SISTEMAS LTDA	Sim	Sim	650	R$ 117,2000	R$ 76.180,0000	14/07/2021 15:47:40
	Marca: Kaspersky **Fabricante:** Kaspersky **Modelo / Versão:** Business Select **Descrição Detalhada do Objeto Ofertado:** Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select. **Porte da empresa:** ME/EPP						
13.497.079/0001-50	ALLSEC SERVICOS EM TECNOLOGIA DA INFORMACAO LTDA	Sim	Sim	650	R$ 117,2000	R$ 76.180,0000	15/07/2021 10:06:41
	Marca: KASPERSKY **Fabricante:** KASPERSKY LAB **Modelo / Versão:** Kaspersky Endpoint Security –Versão Business Selec **Descrição Detalhada do Objeto Ofertado:** Aquisição de licenças do software deantivírus Kaspersky Endpoint Security –Versão Business Select. **Porte da empresa:** ME/EPP						
35.840.944/0001-51	LAZZACLEAN SERVICOS DE PORTARIAS LTDA	Sim	Sim	650	R$ 319,0000	R$ 207.350,0000	15/07/2021 11:55:53
	Marca: KASPERSKY **Fabricante:** KASPERSKY **Modelo / Versão:** ENDPOINT **Descrição Detalhada do Objeto Ofertado:** Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select **Porte da empresa:** ME/EPP						

Lances (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R$ 319,0000	35.840.944/0001-51	15/07/2021 14:00:00:450
R$ 117,2000	13.497.079/0001-50	15/07/2021 14:00:00:450
R$ 117,2000	19.585.941/0001-62	15/07/2021 14:00:00:450
R$ 115,0000	10.224.281/0001-10	15/07/2021 14:00:00:450
R$ 112,0000	10.224.281/0001-10	15/07/2021 14:09:01:233

Não existem lances de desempate ME/EPP para o item

Eventos do Item

Evento	Data	Observações
Abertura	15/07/2021 14:00:03	Item aberto.
Encerramento etapa aberta	15/07/2021 14:11:02	Encerrada etapa aberta do item.
Sorteio eletrônico	15/07/2021 14:11:02	Item teve empate real para o valor 117,2000. Procedeu-se o sorteio eletrônico entre os fornecedores com propostas empatadas.
Encerramento	15/07/2021 14:11:02	Item encerrado.
Abertura do prazo - Convocação anexo	20/07/2021 13:44:51	Convocado para envio de anexo o fornecedor QUALITEK TECNOLOGIA LTDA, CNPJ/CPF: 10.224.281/0001-10.
Encerramento do prazo - Convocação anexo	20/07/2021 13:57:55	Encerrado o prazo de Convocação de Anexo pelo fornecedor QUALITEK TECNOLOGIA LTDA, CNPJ/CPF: 10.224.281/0001-10.
Aceite de proposta	20/07/2021 14:06:23	Aceite individual da proposta. Fornecedor: QUALITEK TECNOLOGIA LTDA, CNPJ/CPF: 10.224.281/0001-10, pelo melhor lance de R$ 112,0000 e com valor negociado a R$ 111,0000. Motivo: Proposta Negociada via CHAT
Habilitação de fornecedor	20/07/2021 14:07:25	Habilitação em grupo de propostas. Fornecedor: QUALITEK TECNOLOGIA LTDA - CNPJ/CPF: 10.224.281/0001-10

Não existem intenções de recurso para o item

Troca de Mensagens

	Data	Mensagem
Sistema	15/07/2021 14:00:00	A sessão pública está aberta. Nesta compra foi realizada a análise de propostas automática e todas foram classificadas para a fase de lances. Até 2 itens poderão estar em disputa simultaneamente e o período de abertura para disputa será entre 08:00 e 18:00. Mantenham-se conectados.
Sistema	15/07/2021 14:00:02	O item 1 foi aberto. Solicitamos o envio de lances.
Sistema	15/07/2021 14:00:03	O item 2 foi aberto. Solicitamos o envio de lances.
Pregoeiro	15/07/2021 14:02:26	Boa Tarde a Todos, Peçamos que se Atentem a todos os Itens do Instrumento Convocatório.
Sistema	15/07/2021 14:10:48	O item 1 teve empate real para o valor 113,1900. Procedeu-se o sorteio eletrônico entre os fornecedores com propostas empatadas. Acompanhe as convocações no Julgamento de Propostas.
Sistema	15/07/2021 14:10:48	O item 1 está encerrado.
Sistema	15/07/2021 14:11:02	O item 2 teve empate real para o valor 117,2000. Procedeu-se o sorteio eletrônico entre os fornecedores com propostas

		empatadas. Acompanhe as convocações no Julgamento de Propostas.
Sistema	15/07/2021 14:11:02	O item 2 está encerrado.
Sistema	15/07/2021 14:11:28	Será iniciada a etapa de Julgamento de Propostas. Favor acompanhar através da funcionalidade "Acompanhar julgamento/habilitação/admissibilidade.
Pregoeiro	15/07/2021 14:22:30	Srs Licitantes, Encerrada a Etapa de Lances, Iniciamos a Etapa de Julgamento, assim a Sessão será suspensa para envio dos autos ao setor demandante, que tão logo seu retorno, reagendaremos uma nova sessão para deliberarmos os feitos
Pregoeiro	15/07/2021 14:22:44	Boa Tarde a Todos!
Pregoeiro	16/07/2021 16:29:38	Sr Licitante, fica Agendado o Retorno da Sessão Referente ao PE 039-2021 para dia 20-07-2021, terça feira as 13:30 (horário de Brasília)
Pregoeiro	16/07/2021 16:32:41	Na Oportunidade, Informamos que a Manifestação Emitida pelo Setor Demandante será Disponibilizada no sitio desta Corte
Pregoeiro	16/07/2021 16:37:29	Informamos ainda que a manifestação emitida pelo setor demandante pode ser acessada no link a seguir: https://sei.tjto.jus.br/sei/documento_consulta_externa.php?id_acesso_externo=58972&id_documento=10000003437916&infra_hash=1b9a174448bac97795909aec8b7917ff
Pregoeiro	20/07/2021 13:30:30	Srs Licitantes, boa Tarde!
Pregoeiro	20/07/2021 13:31:04	Para QUALITEK TECNOLOGIA LTDA - Solicitamos a Empresa Qualitek Tecnologia Ltda, o Envio de uma Contra Proposta Referente aos Itens ora Classificados.
10.224.281/0001-10	20/07/2021 13:37:48	Prezado(a) pregoeiro(a), boa tarde!
10.224.281/0001-10	20/07/2021 13:40:14	Para o item 2, podemos negociar com valor unitário de R$111,00.
Pregoeiro	20/07/2021 13:40:37	Para QUALITEK TECNOLOGIA LTDA - À Empresa Qualitek, Solicitamos o Envio de uma Contra Proposta dos Itens 1 e 2
10.224.281/0001-10	20/07/2021 13:42:24	Para o item 1, podemos negociar com a contra proposta no valor unitário de R$ 107,00.
Pregoeiro	20/07/2021 13:43:16	Para QUALITEK TECNOLOGIA LTDA - ok
Pregoeiro	20/07/2021 13:44:23	Para QUALITEK TECNOLOGIA LTDA - Fica a Empresa Qualitek Convocada a enviar a Proposta Realinhada
Sistema	20/07/2021 13:44:42	Senhor fornecedor QUALITEK TECNOLOGIA LTDA, CNPJ/CPF: 10.224.281/0001-10, solicito o envio do anexo referente ao ítem 1.
Sistema	20/07/2021 13:44:51	Senhor fornecedor QUALITEK TECNOLOGIA LTDA, CNPJ/CPF: 10.224.281/0001-10, solicito o envio do anexo referente ao ítem 2.
10.224.281/0001-10	20/07/2021 13:44:53	Ciente. Obrigado.
Pregoeiro	20/07/2021 13:46:56	Para QUALITEK TECNOLOGIA LTDA - Solicitamos que seja enviado também os dados bancários da empresa pois na proposta inicial não foi observado tal informação
Pregoeiro	20/07/2021 13:50:01	Para QUALITEK TECNOLOGIA LTDA - as informações sobre os dados bancários é o citado no item 5.10 LETRA "B" do edital: a) número do Pregão Eletrônico, identificação social, número do CNPJ responsável pela execução do objeto, assinatura do representante legal da proponente, número de telefone, endereço, dados bancários, e indicação de endereço eletrônico (e-mail); a) número do Preg
Pregoeiro	20/07/2021 13:52:43	Para QUALITEK TECNOLOGIA LTDA - DESCULPAS! CONSEGUIMOS LOCALIZAR AS INFOMAÇÕES BANCÁRIAS NA PROPOSTA INICILA, PORTANTO DESCONSIDERE A SOLICITAÇÃO ANTERIOR!
10.224.281/0001-10	20/07/2021 13:53:27	Sem problemas, ciente. Estamos atualizando a proposta comercial com os novos valores.
Sistema	20/07/2021 13:56:47	Senhor Pregoeiro, o fornecedor QUALITEK TECNOLOGIA LTDA, CNPJ/CPF: 10.224.281/0001-10, enviou o anexo para o ítem 1.
Sistema	20/07/2021 13:57:55	Senhor Pregoeiro, o fornecedor QUALITEK TECNOLOGIA LTDA, CNPJ/CPF: 10.224.281/0001-10, enviou o anexo para o ítem 2.
Sistema	20/07/2021 14:07:25	Srs. Fornecedores, está aberto o prazo para registro de intenção de recursos para os itens/grupos na situação de ´aceito e habilitado´ ou ´cancelado no julgamento´.
Pregoeiro	20/07/2021 14:08:04	Foi informado o prazo final para registro de intenção de recursos: 20/07/2021 às 14:47:00.

Eventos do Pregão

Evento	Data/Hora	Observações
Abertura da sessão pública	15/07/2021 14:00:00	Abertura da sessão pública
Julgamento de propostas	15/07/2021 14:11:28	Início da etapa de julgamento de propostas
Abertura do prazo	20/07/2021 14:07:25	Abertura de prazo para intenção de recurso
Fechamento do prazo	20/07/2021 14:08:04	Fechamento de prazo para registro de intenção de recurso: 20/07/2021 às 14:47:00.

Após encerramento da Sessão Pública, os licitantes melhores classificados foram declarados vencedores dos respectivos itens. Foi divulgado o resultado da Sessão Pública e foi concedido o prazo recursal conforme preconiza o artigo 45, do Decreto 10.024 de 20 de setembro de 2019. Nada mais havendo a declarar, foi encerrada a sessão às 14:49 horas do dia 20 de julho de 2021, cuja ata foi lavrada e assinada pelo Pregoeiro e Equipe de Apoio.

AGNO PAIXAO SARAIVA
Pregoeiro Oficial

GABRIELE BATISTA CRISPIM
Equipe de Apoio

PAULINE SABARA SOUZA
Equipe de Apoio

ENIO CARVALHO DE SOUZA
Equipe de Apoio

Imprimir o **Relatório**

Voltar

OBJETO: Registro de preços visando à aquisição futura de mobiliários para atender as demandas do Poder Judiciário do Estado do Tocantins.
VIGÊNCIA: A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da publicação do extrato no Diário da Justiça Eletrônico - DJE.
DATA DA ASSINATURA: 12 de agosto 2021.

EXTRATO DA ATA DE REGISTRO DE PREÇOS Nº 84/2021
PROCESSO ADMINISTRATIVO 20.0.000024813-5
PREGÃO ELETRÔNICO – SRP Nº 8/2021
ORGÃO GERENCIADOR: Tribunal de Justiça do Estado do Tocantins
FORNECEDOR REGISTRADO: Tecno2000 Indústria e Comércio - Ltda
OBJETO: Registro de preços visando à aquisição futura de mobiliários para atender às demandas do Poder Judiciário do Estado do Tocantins.
VIGÊNCIA: A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da publicação do extrato no Diário da Justiça Eletrônico - DJE.
DATA DA ASSINATURA: 12 de agosto 2021.

EXTRATO DA ATA DE REGISTRO DE PREÇOS Nº 88/2021
PROCESSO ADMINISTRATIVO 20.0.000024813-5
PREGÃO ELETRÔNICO – SRP Nº 8/2021
ORGÃO GERENCIADOR: Tribunal de Justiça do Estado do Tocantins
FORNECEDOR REGISTRADO: Centra Móveis S.A
OBJETO: Registro de preços visando à aquisição futura de mobiliários para atender às demandas do Poder Judiciário do Estado do Tocantins.
VIGÊNCIA: A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da publicação do extrato no Diário da Justiça Eletrônico - DJE.
DATA DA ASSINATURA: 12 de agosto 2021.

EXTRATO DA ATA DE REGISTRO DE PREÇOS Nº 93/2021
PROCESSO ADMINISTRATIVO 21.0.000002638-4
PREGÃO ELETRÔNICO – SRP Nº 39/2021
ORGÃO GERENCIADOR: Tribunal de Justiça do Estado do Tocantins
FORNECEDOR REGISTRADO: Qualitek Tecnologia - Ltda
OBJETO: Registro de preços visando à renovação e a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – Versão Business Select, incluindo atualizações e suporte técnico, com o objetivo de atender às demandas do Poder Judiciário do Estado do Tocantins.
VIGÊNCIA: A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da publicação do extrato no Diário da Justiça Eletrônico - DJE.
DATA DA ASSINATURA: 12 de agosto 2021.

EXTRATO DA ATA DE REGISTRO DE PREÇOS Nº 105/2021
PROCESSO ADMINISTRATIVO 20.0.000025350-3
PREGÃO ELETRÔNICO – SRP Nº 11/2021
ORGÃO GERENCIADOR: Tribunal de Justiça do Estado do Tocantins
FORNECEDOR REGISTRADO: MB Escritórios Inteligentes – Ltda
OBJETO: Registro de preços visando à aquisição futura de mobiliários, poltronas, longarinas e sofás, para atender às demandas do Poder Judiciário do Estado do Tocantins.
VIGÊNCIA: A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da publicação do extrato no Diário da Justiça Eletrônico - DJE.
DATA DA ASSINATURA: 12 de agosto 2021.

EXTRATO DA ATA DE REGISTRO DE PREÇOS Nº 106/2021
PROCESSO ADMINISTRATIVO 20.0.000025350-3
PREGÃO ELETRÔNICO – SRP Nº 11/2021
ORGÃO GERENCIADOR: Tribunal de Justiça do Estado do Tocantins
FORNECEDOR REGISTRADO: Leftec Comércio e Serviços – Ltda
OBJETO: Registro de preços visando à aquisição futura de mobiliários, poltronas e longarinas, para atender às demandas do Poder Judiciário do Estado do Tocantins.
VIGÊNCIA: A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da publicação do extrato no Diário da Justiça Eletrônico - DJE.
DATA DA ASSINATURA: 12 de agosto 2021.

VALOR TOTAL: R$ 384,00 (Trezentos e oitenta e quatro reais).
Unidade Gestora: 060100-FUNJURIS.
Classificação Orçamentária: 0601.02.122.1145.4288
Natureza de Despesa: 33.90.30 – **Subitem:** 36
Fonte de Recursos: 0240
DATA DA EMISSÃO: 23 de junho de 2021.

EXTRATO DE NOTA DE EMPENHO
PROCESSO: 21.0.000013985-5
DISPENSA DE LICITAÇÃO
NOTA DE EMPENHO: 2021NE02030
CONTRATANTE: Fundo Especial de Modernização e Aprimoramento do Poder Judiciário.
CONTRATADA: Elevaenge Comercial e Assistência Técnica em Elevadores LTDA
CNPJ: 09.283.075/0001-00
OBJETO: Empenho destinado à aquisição de peças e/ou componentes para elevadores, com entrega imediata, conforme quantidades e especificações técnicas constantes no Projeto Básico, mediante contratação direta regida pela Lei nº 8.666/93 e suas alterações posteriores, pertinentes aos elevadores existentes nos prédios da sede do Tribunal de Justiça, Escola Superior da Magistratura Tocantinense, e nas Comarcas de Porto Nacional e Guaraí.
VALOR TOTAL: R$ 17.380,00 (Dezessete mil trezentos e oitenta reais).
Unidade Gestora: 060100-FUNJURIS.
Classificação Orçamentária: 0601.02.061.1145.3067
Natureza de Despesa: 33.90.30 – **Subitem:** 99
Fonte de Recursos: 0240
DATA DA EMISSÃO: 24 de junho de 2021.

EXTRATO DE NOTA DE EMPENHO
PROCESSO: 21.0.000013447-0
DISPENSA DE LICITAÇÃO
NOTA DE EMPENHO: 2021NE02098
CONTRATANTE: Fundo Especial de Modernização e Aprimoramento do Poder Judiciário.
CONTRATADA: Croma Equipamentos e Serviços EIRELI
CNPJ: 11.855.692/0001-76
OBJETO: Empenho destinado à aquisição de suprimento de informática (cabeça de impressão – 3 unidades) original, para a impressora plotters HP Designjet T1700, utilizada pela Diretoria de Infraestrutura e Obras do Poder Judiciário do Estado do Tocantins.
VALOR TOTAL: R$ 2.659,92 (Dois mil seiscentos e cinquenta e nove reais e noventa e dois centavos).
Unidade Gestora: 060100-FUNJURIS.
Classificação Orçamentária: 0601.02.126.1145.4231
Natureza de Despesa: 33.90.30 – **Subitem:** 17
Fonte de Recursos: 0240
DATA DA EMISSÃO: 29 de junho de 2021.

COMISSÃO PERMANENTE DE LICITAÇÃO

Avisos de licitações

PREGÃO ELETRÔNICO Nº 042/2021-SRP
AMPLA PARTICIPAÇÃO

Processo nº 21.0.000013200-1- UASG 925814
Modalidade: Pregão Eletrônico nº 042/2021
Tipo: Menor preço por Item
Modo de Disputa: Aberto
Legislação: Lei n º 10.520/2002 - c/c 8.666/93
Objeto: Contratação de empresa especializada visando a aquisição de veículos zero quilômetro.
Disponibilidade do Edital: Dia 02 de julho de 2021. (www.comprasnet.gov.br)
Data da abertura da sessão: Dia 15 de julho de 2021, às 13:30 horas (horário Brasília)
Local: www.comprasgovernamentais.gov.br / Sala da Comissão de Licitação localizada no Edifício Amaro Empresarial, situada na Quadra 103 Norte, Rua NO 11, Lote 2, 7º Andar, Plano Diretor Norte, Palmas/TO, CEP 77.001-036.
Nota: Outras informações na Comissão de Licitação deste Tribunal, pelo telefone (063)3218-4590, das 12:00 às 18:00 horas, ou pela Internet no site *www.tjto.jus.br.*
Palmas – TO, 01 de julho de 2021.

PODER JUDICIÁRIO

TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS

Palácio da Justiça Rio Tocantins, Praça dos Girassóis, sn - Bairro Centro - CEP 77015007 - Palmas - TO - http://wwa.tjto.jus.br
Tribunal de Justiça

Ata de Registro de Preços Nº 93/2021 - PRESIDÊNCIA/DIGER/DIADM/DCC

Processo Administrativo 21.0.000002638-4
Pregão Eletrônico – SRP Nº 39/2021
Validade da Ata: 12 (doze) meses

O **TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS**, inscrito no CNPJ/MF sob o nº 25.053.190/0001-36, com sede na Praça dos Girassóis, s/nº, centro, em Palmas/TO, neste ato representado por o Excelentíssimo Senhor Desembargador **JOÃO RIGO GUIMARÃES**, brasileiro, portador do RG nº 316.531 - SSP/GO, inscrito no CPF/MF sob o nº 056.210.461-53, residente e domiciliado nesta Capital, doravante designado **ÓRGÃO GERENCIADOR**, nos termos da Lei nº 10.520/2002, nº 12.846/2013, pela Lei Complementar nº 123/2006, pelos Decretos nº 10.024/2019, nº 7.892/2013 e nº 8.538/2015 e, subsidiariamente, pela Lei n. 8.666/1993, e demais normas legais aplicáveis, observadas as alterações posteriores introduzidas nos referidos diplomas legais, considerando a classificação das propostas e a respectiva homologação da licitação na modalidade **Pregão Eletrônico para Registro de Preços nº. 39/2021, RESOLVE** registrar os preços da empresa doravante denominada **FORNECEDOR**, nas quantidades estimadas anuais, de acordo com a classificação por ela alcançada por item, atendendo as condições previstas no Instrumento Convocatório e as constantes desta Ata de Registro de Preços, para formação do **SISTEMA DE REGISTRO DE PREÇOS – SRP,** destinado às futuras aquisições sujeitando-se as partes às normas constantes das Leis, Instrução Normativa e Decretos supracitados e em conformidade com as disposições a seguir.

CLÁUSULA PRIMEIRA – DO OBJETO:

1.1. O objeto do presente Instrumento é o registro de preços visando à renovação e a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – Versão Business Select, incluindo atualizações e suporte técnico, com o objetivo de atender às demandas do Poder Judiciário do Estado do Tocantins.

CLÁUSULA SEGUNDA – DO FORNECEDOR REGISTRADO:

2.1. Fornecedor Registrado:

Empresa: Qualitek Tecnologia - Ltda
CNPJ/MF: 10.224.281/0001-10
Endereço: Rua José Ribeiro Dantas, 275, SL 404 e 406, Lagoa Nova, CEP 59062-480, Natal/RN
Telefone: (84) 4008-9454; e-mail: *tecnologia@qualitek.com.br*

Representante: Dennis Fernandes de Medeiros - portador do RG nº 2468043 - ITEP/RN, inscrito no CPF/MF sob o nº 084.417.344-45
Itens: 1 e 2.

CLÁUSULA TERCEIRA – DOS PREÇOS REGISTRADOS:

3.1. Planilha Demonstrativa de Preços:

ITEM	DESCRIÇÕES	UND.	QTDE.	VALOR UNITÁRIO	VALOR TOTAL
1	Renovação de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select, com vigência de 36 (trinta e seis) meses.	Und.	2.850	R$ 107,00	R$ 304.950,00
2	Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select, com vigência de 36 (trinta e seis) meses.	Und.	650	R$ 111,00	R$ 72.150,00
Valor total					**R$ 377.100,00**

3.2. A qualquer tempo, o preço registrado poderá ser revisto em decorrência de eventual redução daqueles existentes no mercado, cabendo ao ÓRGÃO GERENCIADOR convocar o FORNECEDOR registrado para negociar o novo valor, bem como no caso de desequilíbrio-econômico financeiro poderá o FORNECEDOR solicitar revisão dos preços registrados:

3.2.1. A revisão de preços só será admitida no caso de comprovação de desequilíbrio econômico-financeiro, por meio de planilha de custos demonstrativa da majoração e após ampla pesquisa de mercado;

3.2.2. Para a concessão da revisão de preços o FORNECEDOR deverá comunicar ao ÓRGÃO GERENCIADOR, a variação dos preços, por escrito e imediatamente, com pedido justificado de revisão do preço registrado, anexando documentos comprobatórios da majoração e/ou planilha de custos;

3.2.3. Caso o ÓRGÃO GERENCIADOR já tenha emitido a nota de empenho respectiva, para que o FORNECEDOR realize o fornecimento dos objetos, e caso ainda não tenha solicitado a revisão de preços, esta não incidirá sobre o(s) pedido(s) já formalizado(s) e empenhado(s);

3.2.4. O ÓRGÃO GERENCIADOR terá o prazo de 30 (trinta) dias, a partir do recebimento do pleito, para análise dos pedidos de revisão recebidos;

3.2.5. Durante esse período o FORNECEDOR deverá efetuar o fornecimento dos objetos pelo preço registrado e no prazo ajustado, mesmo que a revisão seja julgada procedente pelo ÓRGÃO GERENCIADOR. Nesse caso, o ÓRGÃO GERENCIADOR procederá ao reforço dos valores pertinentes aos quantitativos dos objetos empenhadas após a revisão;

3.2.6. O FORNECEDOR obrigar-se-á realizar o fornecimento dos objetos pelo preço registrado caso o pedido de revisão seja julgado improcedente;

3.2.7. Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao preço praticado no mercado o ÓRGÃO GERENCIADOR convocará o FORNECEDOR visando à negociação para redução de preços e sua adequação ao praticado no mercado;

3.2.7.1. Frustrada a negociação, o FORNECEDOR será liberado do compromisso assumido;

3.2.8. Quando o preço de mercado tornar-se superior aos preços registrados e o FORNECEDOR, mediante requerimento devidamente comprovado, não puder cumprir o compromisso, o ÓRGÃO GERENCIADOR poderá liberar o FORNECEDOR da obrigação assumida, sem aplicação de penalidade, confirmando a veracidade dos motivos e comprovantes apresentados, desde que a comunicação ocorra antes do pedido de fornecimento;

3.2.9. Em qualquer hipótese, os preços decorrentes da revisão não poderão ultrapassar os praticados no mercado, mantendo-se a diferença percentual apurado entre o valor originalmente constante da proposta do FORNECEDOR é aquela vigente no mercado à época do registro – equação econômico-financeiro;

3.2.10. Será considerado preço de mercado o que for igual ou inferior à média daqueles apurados pelo ÓRGÃO GERENCIADOR para o objeto pesquisado.

CLÁUSULA QUARTA – DA VIGÊNCIA DA ATA:

4.1. A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da publicação do extrato no Diário da Justiça Eletrônico - DJE.

4.2. Esta Ata de Registro de Preços com a indicação do FORNECEDOR e Preços Registrados será divulgada no site: http://www.tjto.jus.br / (http://www.tjto.jus.br/index.php/cidadao/licitacoes) e ficará disponibilizada durante sua vigência, que será nós termos do item 4.1.

CLÁUSULA QUINTA – DA VINCULAÇÃO:

5.1. As especificações constantes nesta Ata de Registro de Preços vinculam-se aos autos nº. 21.0.000002638-4, do qual é parte integrante e complementar independentemente de transcrição.

CLÁUSULA SEXTA – DO CANCELAMENTO DO REGISTRO DE PREÇOS:

6.1. O registro do FORNECEDOR poderá ser cancelado, garantida a prévia defesa, no prazo de 5 (cinco) dias úteis, a contar do recebimento da notificação, nas seguintes hipóteses:

6.1.1. Pelo ÓRGÃO GERENCIADOR, quando:

a) O FORNECEDOR não cumprir as exigências contidas nesta Ata de Registro de Preços, Edital de Licitação e contratos firmados;

b) O FORNECEDOR der causa à rescisão administrativa, da contratação decorrente deste Registro de Preços, por um dos motivos elencados no art. 78 e seus incisos da Lei nº. 8.666/93, alterada pela Lei nº 8.883/94;

c) O FORNECEDOR não aceitar reduzir o seu preço registrado, quando este se apresentar superior ao praticado pelo mercado;

d) por razões de interesse público, devidamente fundamentadas, na forma do inciso XII, do art. 78 da Lei nº. 8.666/93, alterada pela Lei nº. 8.883/94;

6.2. A pedido do FORNECEDOR quando:

a) Mediante solicitação por escrito, comprovar estar impossibilitado de cumprir as obrigações/exigências assumidas por meio desta Ata de Registro de Preços.

6.3. O cancelamento será precedido de processo administrativo, sendo que a decisão final deverá ser fundamentada.

6.4. A comunicação do cancelamento do registro do FORNECEDOR será feita por escrito, juntando-se o comprovante de recebimento.

6.5. No caso do FORNECEDOR encontrar-se em lugar ignorado, incerto ou inacessível, a comunicação será feita por publicação, no Diário da Justiça Eletrônico - DJE, considerando-se cancelado o registro do FORNECEDOR, a partir do 5º (quinto) dia útil, a contar da publicação; e

6.6. A solicitação do FORNECEDOR para cancelamento do registro de preço, não o desobriga do fornecimento dos objetos, até a decisão final do ÓRGÃO GERENCIADOR, a qual deverá ser prolatada no prazo máximo de 30 (trinta) dias, facultado o ÓRGÃO GERENCIADOR a aplicação das penalidades previstas nesta Ata e no Instrumento convocatório, caso não aceitas as razões do pedido.

CLÁUSULA SÉTIMA – DA FORMAÇÃO DO CADASTRO DE RESERVA:

7.1. Após o encerramento da sessão e declarada a vencedora do certame, as demais licitantes poderão reduzir seus preços ao valor da proposta da licitante declarada vencedora, com vistas a formação do cadastro de reserva.

7.2. A manifestação em integrar o cadastro de reserva não altera o resultado do certame, cabendo apenas aos itens com propostas adjudicadas.

7.3. O licitante que compuser o cadastro de reserva disposto no item 7.2, será convocado em caso de cancelamento do registro de preços do 1º (primeiro) colocado, nas hipóteses previstas nos arts. 20 e 21 do Decreto n.º 7.892/13.

7.4. Se mais de um licitante manifestar interesse em compor o cadastro de reserva a que se refere o item 7.2, os mesmos serão classificados segundo a ordem da última proposta apresentada na etapa de lances, excluídos o percentual referente à margem de preferência, quando o objeto não atender o disposto no art. 3º da Lei n.º 8.666/93.

7.5. Uma vez cancelado o registro de preços nos termos do item 7.2, a autoridade competente, convocará os participantes do certame, designando o dia e hora para realização da habilitação dos fornecedores que comporão o cadastro de reserva, observados a ordem de classificação.

7.6. A recusa injustificada do fornecedor classificado em assinar a ata, dentro do prazo estabelecido no item 7.4, ensejará a aplicação de penalidades descritas no item 18 do Edital de Licitação.

7.7. A contratação formalizar-se-á mediante instrumento particular, observadas as cláusulas e condições do Edital, da Ata de Registro de Preços e da proposta vencedora.

7.8. A licitante que tenha seu preço registrado estará obrigada a cumprir todas as condições dispostas nesta Ata de Registro de Preços.

CLÁUSULA OITAVA – DA ADESÃO À ATA DE REGISTRO DE PREÇOS:

8.1. Caberá ao órgão aderente à Ata de Registro de Preços, verificar junto ao FORNECEDOR a capacidade de fornecimento dos objetos, bem como consultar o ÓRGÃO GERENCIADOR sobre a sua anuência.

8.2. Caberá ao FORNECEDOR, observadas as condições estabelecidas, optar pela aceitação do fornecimento dos objetos, desde que não venha a prejudicar as obrigações anteriormente assumidas.

8.3. Os fornecimentos adicionais não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos de cada item do instrumento convocatório e registrado nesta Ata do ÓRGÃO GERENCIADOR e dos órgãos participantes.

8.4. O quantitativo de que trata o item 8.3, não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços do ÓRGÃO GERENCIADOR e da ata de registro de preços dos órgãos participantes, independente do número de órgão não participantes que aderirem.

8.5. Realizada a contratação/aquisição da totalidade do(s) item(ns) registrados para o ÓRGÃO GERENCIADOR não será possível à adesão desta Ata por órgão ou entidade.

CLÁUSULA NONA – DA FORMA DE AQUISIÇÃO:

9.1. As aquisições dos objetos decorrentes do Registro de Preços serão realizadas de acordo com a necessidade e conveniência do ÓRGÃO GERENCIADOR, mediante a emissão de contrato ou somente de nota de empenho, conforme for o caso.

9.2. Os quantitativos dos objetos a serem fornecidos são de livre escolha do ÓRGÃO GERENCIADOR e estarão diretamente vinculados às especificidades constantes nesta Ata.

9.3. A existência de preços registrados não obriga o ÓRGÃO GERENCIADOR a adquiri-los em sua totalidade, e sim promover a aquisição de acordo com suas necessidades, obedecida à legislação pertinente, sendo assegurada ao detentor do registro a preferência em igualdade de condições.

CLÁUSULA DÉCIMA – DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS:

10.1. Renovação de licenças de solução corporativa de antivírus

10.1.1. Características Gerais:

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

10.1.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

10.1.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

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

10.1.2. Servidor de Administração e Console Administrativa

10.1.2.1. Compatibilidade:

10.1.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

10.1.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

10.1.2.1.3. Microsoft Windows Server 2016 x64.

10.1.2.1.4. Microsoft Windows Server 2019 x64.

10.1.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

10.1.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

10.1.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

10.1.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

10.1.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

10.1.2.2. Características:

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

10.1.2.2.2. Console deve ser baseada no modelo cliente/servidor.

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

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

10.1.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

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

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

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

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

10.1.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

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

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

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

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

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

10.1.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

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

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

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

10.1.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

10.1.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

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

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

10.1.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

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

10.1.2.2.25.1. Nome do computador.

10.1.2.2.25.2. Nome do domínio.

10.1.2.2.25.3. Range de IP.

10.1.2.2.25.4. Sistema Operacional.

10.1.2.2.25.5. Máquina virtual.

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

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

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

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

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

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

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

10.1.2.2.33. Deve fornecer as seguintes informações dos computadores:

10.1.2.2.33.1. Se o antivírus está instalado.

10.1.2.2.33.2. Se o antivírus está iniciado.

10.1.2.2.33.3. Se o antivírus está atualizado.

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

10.1.2.2.33.5. Minutos/horas desde a última atualização de vacinas.

10.1.2.2.33.6. Data e horário da última verificação executada na máquina.

10.1.2.2.33.7. Versão do antivírus instalado na máquina.

10.1.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças.

10.1.2.2.33.9. Data e horário de quando a máquina foi ligada.

10.1.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina.

10.1.2.2.33.11. Nome do computador.

10.1.2.2.33.12. Domínio ou grupo de trabalho do computador.

10.1.2.2.33.13. Data e horário da última atualização de vacinas.

10.1.2.2.33.14. Sistema operacional com Service Pack.

101.1.2.2.33.15. Quantidade de processadores.

10.1.2.2.33.16. Quantidade de memória RAM.

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

10.1.2.2.33.18. Endereço IP.

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

10.1.2.2.33.20. Atualizações do Windows Updates instaladas.

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

10.1.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina.

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

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

10.1.2.2.35.1. Alteração de Gateway Padrão.

10.1.2.2.35.2. Alteração de subrede.

2.1.2.2.35.3. Alteração de domínio.

10.1.2.2.35.4. Alteração de servidor DHCP.

10.1.2.2.35.5. Alteração de servidor DNS.

10.1.2.2.35.6. Alteração de servidor WINS.

10.1.2.2.35.7. Alteração de subrede.

10.1.2.2.35.8. Resolução de Nome.

10.1.2.2.35.9. Disponibilidade de endereço de conexão SSL.

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

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

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

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

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

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

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

10.1.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos.

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

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

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

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

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

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

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

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

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

10.1.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

10.1.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

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

10.1.2.2.55.1. Nome do vírus.

10.1.2.2.55.2. Nome do arquivo infectado.

10.1.2.2.55.3. Data e hora da detecção.

10.1.2.2.55.4. Nome da máquina ou endereço IP.

10.1.2.2.55.5. Ação realizada.

10.1.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

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

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

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

10.1.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente.

10.1.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

10.1.3. Estações Windows

10.1.3.1. Compatibilidade:

10.1.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate.

10.1.3.1.2. Microsoft Windows 8 Professional/Enterprise.

10.1.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

10.1.3.1.4. Microsoft Windows 10 Professional/Enterprise.

10.1.3.2. Características:

10.1.3.2.1. Deve prover as seguintes proteções:

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

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

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

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

10.1.3.2.1.5. Firewall com IDS.

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

10.1.3.2.1.7. Controle de dispositivos externos.

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

10.1.3.2.1.9. Controle de acesso a sites por horário.

10.1.3.2.1.10. Controle de acesso a sites por usuários.

10.1.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

10.1.3.2.1.12. Controle de execução de aplicativos.

10.1.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

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

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

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

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

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

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

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

10.1.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

10.1.3.2.12. Capacidade de verificar objetos usando heurística.

10.1.3.2.13. Capacidade de agendar uma pausa na verificação.

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

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

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

10.1.3.2.16.1. Perguntar o que fazer, ou;

10.1.3.2.16.2. Bloquear acesso ao objeto.

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

10.1.3.2.16.2.2. Caso positivo de desinfecção:

10.1.3.2.16.2.2.1. Restaurar o objeto para uso.

10.1.3.2.16.2.3. Caso negativo de desinfecção:

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

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

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

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

10.1.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

10.1.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

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

10.1.3.2.22.1. Perguntar o que fazer, ou;

10.1.3.2.22.2. Bloquear o e-mail.

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

10.1.3.2.22.2.2. Caso positivo de desinfecção:

10.1.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

10.1.3.2.22.2.3. Caso negativo de desinfecção:

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

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

10.1.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

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

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

10.1.3.2.27. Deve ter suporte total ao protocolo Ipv6.

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

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

10.1.3.2.29.1. Perguntar o que fazer, ou;

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

10.1.3.2.29.3. Permitir acesso ao objeto.

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

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

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

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

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

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

10.1.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

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

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

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

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

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

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

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

10.1.3.2.39.1. Discos de armazenamento locais.

10.1.3.2.39.2. Armazenamento removível.

10.1.3.2.39.3. Impressoras.

10.1.3.2.39.4. CD/DVD.

10.1.3.2.39.5. Drives de disquete.

10.1.3.2.39.6. Modems.

10.1.3.2.39.7. Dispositivos de fita.

10.1.3.2.39.8. Dispositivos multifuncionais.

10.1.3.2.39.9. Leitores de smart card.

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

10.1.3.2.39.11. Wi-Fi.

10.1.3.2.39.12. Adaptadores de rede externos.

10.1.3.2.39.13. Dispositivos MP3 ou smartphones.

10.1.3.2.39.14. Dispositivos Bluetooth.

10.1.3.2.39.15. Câmeras e Scanners.

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

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

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

10.1.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

10.1.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

10.1.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

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

10.1.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

10.1.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

10.1.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

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

10.1.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

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

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

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

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

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

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

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

10.1.4. Estações Mac OS X

10.1.4.1. Compatibilidade:

10.1.4.1.1. OS X 10.9 (Mavericks).

10.1.4.1.2. OS X 10.10 (Yosemite).

10.1.4.1.3. OS X 10.11 (El Capitan).

10.1.4.1.4. macOS 10.12 (Sierra).

10.1.4.1.5. macOS 10.13 (High Sierra).

10.1.4.1.6. macOS 10.14 (Mojave).

10.1.4.1.7. macOS 10.15 (Catalina).

10.1.4.1.8. macOS 11.0 (Big Sur).

10.1.4.2. Características:

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

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

10.1.4.2.3. Possuir módulo de bloqueio a ataques na rede.

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

10.1.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

10.1.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

10.1.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

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

10.1.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

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

10.1.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

10.1.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

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

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

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

10.1.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

10.1.4.2.17. Capacidade de verificar objetos usando heurística.

10.1.4.2.18. Capacidade de agendar uma pausa na verificação.

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

10.1.4.2.19.1. Perguntar o que fazer, ou;

10.1.4.2.19.2. Bloquear acesso ao objeto.

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

10.1.4.2.19.3.1. Caso positivo de desinfecção:

10.1.4.2.19.3.1.1. Restaurar o objeto para uso.

10.1.4.2.19.3.2. Caso negativo de desinfecção:

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

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

10.1.4.2.21. Capacidade de verificar arquivos de formato de email.

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

10.1.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

10.1.5. Estações Linux

10.1.5.1. Compatibilidade:

10.1.5.1.1. Plataforma 32 bits:

10.1.5.1.1.1. Ubuntu 16.04 LTS

10.1.5.1.1.2. Red Hat® Enterprise Linux® 6.7

10.1.5.1.1.3. CentOS-6.7

10.1.5.1.1.4. Debian GNU / Linux 9.4

10.1.5.1.2. Plataforma 64 bits:

10.1.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

10.1.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

10.1.5.1.2.3. CentOS-6.7, 7.2, 8.0

10.1.5.1.2.4. Debian GNU / Linux 9.4, 10.1

10.1.5.1.2.5. OracleLinux 7.3, 8

10.1.5.1.2.6. SUSE® Linux Enterprise Server 15

10.1.5.1.2.7. openSUSE® 15

10.1.5.1.2.8. Amazon Linux AMI

10.1.5.2. Características:

10.1.5.2.1. Deve prover as seguintes proteções:

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

10.1.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

10.1.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

10.1.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

10.1.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

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

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

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

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

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

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

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

10.1.5.2.13.1. Alta.

10.1.5.2.13.2. Média.

10.1.5.2.13.3. Baixa.

10.1.5.2.13.4. Recomendado.

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

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

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

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

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

10.1.5.2.19. Capacidade de verificar objetos usando heurística.

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

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

10.1.6. Servidores Windows

10.1.6.1. Compatibilidade:

10.1.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

10.1.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

10.1.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

10.1.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

10.1.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

10.1.6.1.6. Microsoft Windows Server 2016.

10.1.6.1.7. Microsoft Windows Server 2019.

10.1.6.2. Características:

10.1.6.2.1. Deve prover as seguintes proteções:

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

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

10.1.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

10.1.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

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

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

10.1.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

10.1.6.2.4.3. Leitura de configurações.

10.1.6.2.4.4. Modificação de configurações.

10.1.6.2.4.5. Gerenciamento de Backup e Quarentena.

10.1.6.2.4.6. Visualização de relatórios.

10.1.6.2.4.7. Gerenciamento de relatórios.

10.1.6.2.4.8. Gerenciamento de chaves de licença.

10.1.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

10.1.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

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

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

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

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

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

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

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

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

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

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

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

10.1.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

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

10.1.6.2.19. Capacidade de verificar objetos usando heurística.

10.1.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

10.1.6.2.21. Capacidade de agendar uma pausa na verificação.

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

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

10.1.6.2.23.1. Perguntar o que fazer, ou;

10.1.6.2.23.2. Bloquear acesso ao objeto.

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

10.1.6.2.23.2.2. Caso positivo de desinfecção:

10.1.6.2.23.2.2.1. Restaurar o objeto para uso.

10.1.6.2.23.3. Caso negativo de desinfecção:

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

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

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

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

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

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

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

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

10.1.7. Servidores Linux

10.1.7.1. Compatibilidade:

10.1.7.1.1. Plataforma 32 bits:

10.1.7.1.1.1. Ubuntu 16.04 LTS.

10.1.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

10.1.7.1.1.3. CentOS-6.7.

10.1.7.1.1.4. Debian GNU / Linux 9.4.

10.1.7.1.2. Plataforma 64 bits:

10.1.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

10.1.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

10.1.7.1.2.3. CentOS-6.7, 7.2, 8.0.

10.1.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

10.1.7.1.2.5. OracleLinux 7.3, 8.

10.1.7.1.2.6. SUSE® Linux Enterprise Server 15.

10.1.7.1.2.7. openSUSE® 15.

10.1.7.1.2.8. Amazon Linux AMI.

10.1.7.2. Características:

10.1.7.2.1. Deve prover as seguintes proteções:

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

10.1.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

10.1.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

10.1.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

10.1.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

2.1.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

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

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

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

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

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

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

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

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

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

10.1.7.2.7. Capacidade de verificar objetos usando heurística.

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

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

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

10.1.8. Smartphones e tablets

10.1.8.1. Compatibilidade:

10.1.8.1.1. Dispositivos com os sistemas operacionais:

10.1.8.1.1.1. Android 4.2 – 11.

10.1.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

10.1.8.2. Características:

10.1.8.2.1. Deve prover as seguintes proteções:

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

10.1.8.2.1.2. Proteção contra adware e autodialers.

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

10.1.8.2.1.4. Arquivos abertos no smartphone.

10.1.8.2.1.5. Programas instalados usando a interface do smartphone

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

10.1.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

10.1.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

10.1.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

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

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

10.1.8.2.7. Deverá ter firewall pessoal (Android).

10.1.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

10.1.8.2.9. Capacidade de enviar comandos remotamente de:

10.1.8.2.9.1. Localizar.

10.1.8.2.9.2. Bloquear.

10.1.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

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

10.1.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

10.1.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

10.1.8.2.14. Capacidade de localizar o dispositivo quando necessário.

10.1.8.2.15. Permitir atualização das definições quando estiver em "roaming".

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

10.1.8.2.17. Deve permitir verificar somente arquivos executáveis.

10.1.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

10.1.8.2.19. Capacidade de agendar uma verificação.

10.1.8.2.20. Capacidade de enviar URL de instalação por e-mail.

10.1.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

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

10.1.8.2.22.1. Deletar.

10.1.8.2.22.2. Ignorar.

10.1.8.2.22.3. Quarentenar.

10.1.8.2.22.4. Perguntar ao usuário.

10.1.9. Gerenciamento de dispositivos móveis (MDM):

10.1.9.1. Compatibilidade:

10.1.9.1.1. Android 4.2 – 11.

10.1.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

10.1.9.2. Características:

10.1.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

10.1.9.2.2. Capacidade de ajustar as configurações de:

10.1.9.2.2.1. Sincronização de e-mail.

10.1.9.2.2..2. Uso de aplicativos.

10.1.9.2.2.3. Senha do usuário.

10.1.9.2.2.4. Criptografia de dados.

10.1.9.2.2.5. Conexão de mídia removível.

10.1.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

10.1.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

10.1.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

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

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

10.1.9.2.8. Permitir sincronização com perfil do "Touch Down".

10.1.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

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

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

10.2. Aquisição de licenças de solução corporativa de antivírus

10.2.1. Características Gerais

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

10.2.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

10.2.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

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

10.2.2. Servidor de Administração e Console Administrativa

10.2.2.1. Compatibilidade:

10.2.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

10.2.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

10.2.2.1.3. Microsoft Windows Server 2016 x64.

10.2.2.1.4. Microsoft Windows Server 2019 x64.

10.2.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

10.2.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

10.2.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

10.2.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

10.2.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

10.2.2.2. Características:

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

10.2.2.2.2. Console deve ser baseada no modelo cliente/servidor.

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

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

10.2.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

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

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

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

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

10.2.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

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

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

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

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

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

10.2.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

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

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

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

10.2.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

10.2.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

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

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

10.2.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

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

10.2.2.2.25.1. Nome do computador.

10.2.2.2.25.2. Nome do domínio.

10.2.2.2.25.3. Range de IP.

10.2.2.2.25.4. Sistema Operacional.

10.2.2.2.25.5. Máquina virtual.

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

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

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

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

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

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

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

10.2.2.2.33. Deve fornecer as seguintes informações dos computadores:

10.2.2.2.33.1. Se o antivírus está instalado.

10.2.2.2.33.2. Se o antivírus está iniciado.

10.2.2.2.33.3. Se o antivírus está atualizado.

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

10.2.2.2.33.5. Minutos/horas desde a última atualização de vacinas.

10.2.2.2.33.6. Data e horário da última verificação executada na máquina.

10.2.2.2.33.7. Versão do antivírus instalado na máquina.

10.2.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças.

10.2.2.2.33.9. Data e horário de quando a máquina foi ligada.

10.2.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina.

10.2.2.2.33.11. Nome do computador.

10.2.2.2.33.12. Domínio ou grupo de trabalho do computador.

10.2.2.2.33.13. Data e horário da última atualização de vacinas.

10.2.2.2.33.14. Sistema operacional com Service Pack.

10.2.2.2.33.15. Quantidade de processadores.

10.2.2.2.33.16. Quantidade de memória RAM.

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

10.2.2.2.33.18. Endereço IP.

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

10.2.2.2.33.20. Atualizações do Windows Updates instaladas.

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

10.2.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina.

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

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

10.2.2.2.35.1. Alteração de Gateway Padrão.

10.2.2.2.35.2. Alteração de subrede.

10.2.2.2.35.3. Alteração de domínio.

10.2.2.2.35.4. Alteração de servidor DHCP.

10.2.2.2.35.5. Alteração de servidor DNS.

10.2.2.2.35.6. Alteração de servidor WINS.

10.2.2.2.35.7. Alteração de subrede.

10.2.2.2.35.8. Resolução de Nome.

10.2.2.2.35.9. Disponibilidade de endereço de conexão SSL.

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

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

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

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

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

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

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

10.2.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos.

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

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

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

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

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

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

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

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

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

10.2.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

10.2.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

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

10.2.2.2.55.1. Nome do vírus.

10.2.2.2.55.2. Nome do arquivo infectado.

10.2.2.2.55.3. Data e hora da detecção.

10.2.2.2.55.4. Nome da máquina ou endereço IP.

10.2.2.2.55.5. Ação realizada.

10.2.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

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

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

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

10.2.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente.

10.2.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

10.2.3. Estações Windows

10.2.3.1. Compatibilidade:

10.2.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate.

10.2.3.1.2. Microsoft Windows 8 Professional/Enterprise.

10.2.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

10.2.3.1.4. Microsoft Windows 10 Professional/Enterprise.

10.2.3.2. Características:

10.2.3.2.1. Deve prover as seguintes proteções:

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

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

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

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

10.2.3.2.1.5. Firewall com IDS.

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

10.2.3.2.1.7. Controle de dispositivos externos.

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

10.2.3.2.1.9. Controle de acesso a sites por horário.

10.2.3.2.1.10. Controle de acesso a sites por usuários.

10.2.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

10.2.3.2.1.12. Controle de execução de aplicativos.

10.2.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

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

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

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

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

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

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

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

10.2.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

10.2.3.2.12. Capacidade de verificar objetos usando heurística.

10.2.3.2.13. Capacidade de agendar uma pausa na verificação.

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

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

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

10.2.3.2.16.1. Perguntar o que fazer, ou;

10.2.3.2.16.2. Bloquear acesso ao objeto.

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

10.2.3.2.16.2.2. Caso positivo de desinfecção:

10.2.3.2.16.2.2.1. Restaurar o objeto para uso.

10.2.3.2.16.2.3. Caso negativo de desinfecção:

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

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

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

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

10.2.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

10.2.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

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

10.2.3.2.22.1. Perguntar o que fazer, ou;

10.2.3.2.22.2. Bloquear o e-mail.

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

10.2.3.2.22.2.2. Caso positivo de desinfecção:

10.2.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

10.2.3.2.22.2.3. Caso negativo de desinfecção:

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

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

10.2.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

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

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

10.2.3.2.27. Deve ter suporte total ao protocolo Ipv6.

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

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

10.2.3.2.29.1. Perguntar o que fazer, ou;

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

10.2.3.2.29.3. Permitir acesso ao objeto.

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

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

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

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

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

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

10.2.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

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

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

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

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

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

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

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

10.2.3.2.39.1. Discos de armazenamento locais.

10.2.3.2.39.2. Armazenamento removível.

10.2.3.2.39.3. Impressoras.

10.2.3.2.39.4. CD/DVD.

10.2.3.2.39.5. Drives de disquete.

10.2.3.2.39.6. Modems.

10.2.3.2.39.7. Dispositivos de fita.

10.2.3.2.39.8. Dispositivos multifuncionais.

10.2.3.2.39.9. Leitores de smart card.

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

10.2.3.2.39.11. Wi-Fi.

10.2.3.2.39.12. Adaptadores de rede externos.

10.2.3.2.39.13. Dispositivos MP3 ou smartphones.

10.2.3.2.39.14. Dispositivos Bluetooth.

10.2.3.2.39.15. Câmeras e Scanners.

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

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

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

10.2.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

10.2.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

10.2.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

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

10.2.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

10.2.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

10.2.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

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

10.2.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

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

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

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

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

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

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

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

10.2.4. Estações Mac OS X

10.2.4.1. Compatibilidade:

10.2.4.1.1. OS X 10.9 (Mavericks).

10.2.4.1.2. OS X 10.10 (Yosemite).

10.2.4.1.3. OS X 10.11 (El Capitan).

10.2.4.1.4. macOS 10.12 (Sierra).

10.2.4.1.5. macOS 10.13 (High Sierra).

10.2.4.1.6. macOS 10.14 (Mojave).

10.2.4.1.7. macOS 10.15 (Catalina).

10.2.4.1.8. macOS 11.0 (Big Sur).

10.2.4.2. Características:

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

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

10.2.4.2.3. Possuir módulo de bloqueio a ataques na rede.

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

10.2.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

10.2.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

10.2.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

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

10.2.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

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

10.2.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

10.2.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

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

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

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

10.2.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

10.2.4.2.17. Capacidade de verificar objetos usando heurística.

10.2.4.2.18. Capacidade de agendar uma pausa na verificação.

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

10.2.4.2.19.1. Perguntar o que fazer, ou;

10.2.4.2.19.2. Bloquear acesso ao objeto.

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

10.2.4.2.19.3.1. Caso positivo de desinfecção:

10.2.4.2.19.3.1.1. Restaurar o objeto para uso.

10.2.4.2.19.3.2. Caso negativo de desinfecção:

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

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

10.2.4.2.21. Capacidade de verificar arquivos de formato de email.

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

10.2.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

10.2.5. Estações Linux

10.2.5.1. Compatibilidade:

10.2.5.1.1. Plataforma 32 bits:

10.2.5.1.1.1. Ubuntu 16.04 LTS

10.2.5.1.1.2. Red Hat® Enterprise Linux® 6.7

10.2.5.1.1.3. CentOS-6.7

10.2.5.1.1.4. Debian GNU / Linux 9.4

10.2.5.1.2. Plataforma 64 bits:

10.2.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

10.2.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

10.2.5.1.2.3. CentOS-6.7, 7.2, 8.0

10.2.5.1.2.4. Debian GNU / Linux 9.4, 10.1

10.2.5.1.2.5. OracleLinux 7.3, 8

10.2.5.1.2.6. SUSE® Linux Enterprise Server 15

10.2.5.1.2.7. openSUSE® 15

10.2.5.1.2.8. Amazon Linux AMI

10.2.5.2. Características

10.2.5.2.1. Deve prover as seguintes proteções:

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

10.2.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

10.2.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

10.2.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

10.2.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

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

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

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

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

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

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

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

10.2.5.2.13.1. Alta.

10.2.5.2.13.2. Média.

10.2.5.2.13.3. Baixa.

10.2.5.2.13.4. Recomendado.

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

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

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

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

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

10.2.5.2.19. Capacidade de verificar objetos usando heurística.

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

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

10.2.6. Servidores Windows

10.2.6.1. Compatibilidade:

10.2.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

10.2.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

10.2.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

10.2.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

10.2.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

10.2.6.1.6. Microsoft Windows Server 2016.

10.2.6.1.7. Microsoft Windows Server 2019.

10.2.6.2. Características:

10.2.6.2.1. Deve prover as seguintes proteções:

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

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

10.2.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

10.2.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

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

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

10.2.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

10.2.6.2.4.3. Leitura de configurações.

10.2.6.2.4.4. Modificação de configurações.

10.2.6.2.4.5. Gerenciamento de Backup e Quarentena.

10.2.6.2.4.6. Visualização de relatórios.

10.2.6.2.4.7. Gerenciamento de relatórios.

10.2.6.2.4.8. Gerenciamento de chaves de licença.

10.2.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

10.2.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

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

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

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

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

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

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

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

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

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

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

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

10.2.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

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

10.2.6.2.19. Capacidade de verificar objetos usando heurística.

10.2.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

10.2.6.2.21. Capacidade de agendar uma pausa na verificação.

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

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

10.2.6.2.23.1. Perguntar o que fazer, ou;

10.2.6.2.23.2. Bloquear acesso ao objeto.

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

10.2.6.2.23.2.2. Caso positivo de desinfecção:

10.2.6.2.23.2.2.1. Restaurar o objeto para uso.

10.2.6.2.23.3. Caso negativo de desinfecção:

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

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

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

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

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

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

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

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

10.2.7. Servidores Linux

10.2.7.1. Compatibilidade:

10.2.7.1.1. Plataforma 32 bits:

10.2.7.1.1.1. Ubuntu 16.04 LTS.

10.2.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

10.2.7.1.1.3. CentOS-6.7.

10.2.7.1.1.4. Debian GNU / Linux 9.4.

10.2.7.1.2. Plataforma 64 bits:

10.2.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

10.2.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

10.2.7.1.2.3. CentOS-6.7, 7.2, 8.0.

10.2.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

10.2.7.1.2.5. OracleLinux 7.3, 8.

10.2.7.1.2.6. SUSE® Linux Enterprise Server 15.

10.2.7.1.2.7. openSUSE® 15.

10.2.7.1.2.8. Amazon Linux AMI.

10.2.7.2. Características:

10.2.7.2.1. Deve prover as seguintes proteções:

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

10.2.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

10.2.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

10.2.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

10.2.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

10.2.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

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

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

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

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

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

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

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

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

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

10.2.7.2.7. Capacidade de verificar objetos usando heurística.

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

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

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

10.2.8. Smartphones e tablets

10.2.8.1. Compatibilidade:

10.2.8.1.1. Dispositivos com os sistemas operacionais:

10.2.8.1.1.1. Android 4.2 – 11.

10.2.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

10.2.8.2. Características:

10.2.8.2.1. Deve prover as seguintes proteções:

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

10.2.8.2.1.2. Proteção contra adware e autodialers.

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

10.2.8.2.1.4. Arquivos abertos no smartphone.

10.2.8.2.1.5. Programas instalados usando a interface do smartphone

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

10.2.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

10.2.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

10.2.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

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

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

10.2.8.2.7. Deverá ter firewall pessoal (Android).

10.2.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

10.2.8.2.9. Capacidade de enviar comandos remotamente de:

10.2.8.2.9.1. Localizar.

10.2.8.2.9.2. Bloquear.

10.2.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

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

10.2.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

10.2.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

10.2.8.2.14. Capacidade de localizar o dispositivo quando necessário.

10.2.8.2.15. Permitir atualização das definições quando estiver em "roaming".

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

10.2.8.2.17. Deve permitir verificar somente arquivos executáveis.

10.2.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

10.2.8.2.19. Capacidade de agendar uma verificação.

10.2.8.2.20. Capacidade de enviar URL de instalação por e-mail.

10.2.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

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

10.2.8.2.22.1. Deletar.

10.2.8.2.22.2. Ignorar.

10.2.8.2.22.3. Quarentenar.

10.2.8.2.22.4. Perguntar ao usuário.

10.2.9. Gerenciamento de dispositivos móveis (MDM):

10.2.9.1. Compatibilidade:

10.2.9.1.1. Android 4.2 – 11.

10.2.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

10.2.9.2. Características:

10.2.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

10.2.9.2.2. Capacidade de ajustar as configurações de:

10.2.9.2.2.1. Sincronização de e-mail.

10.2.9.2.2..2. Uso de aplicativos.

10.2.9.2.2.3. Senha do usuário.

10.2.9.2.2.4. Criptografia de dados.

10.2.9.2.2.5. Conexão de mídia removível.

10.2.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

10.2.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

10.2.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

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

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

10.2.9.2.8. Permitir sincronização com perfil do "Touch Down".

10.2.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

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

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

10.3. Transferência de conhecimento e direitos de propriedade intelectual

10.3.1. O uso de uma solução de antivírus corporativo é imprescindível por conter funções de proteção que vão além de um antivírus comum, evitando, portanto, invasões ou roubos de informações, por exemplo. Por isso, não existe versões corporativas gratuitas, não sendo vislumbrada outra forma de utilização senão a obrigatoriedade da renovação/aquisição dessa tecnologia de terceiros.

10.3.2. Os antivírus corporativos são produtos consolidados no mercado de Tecnologia da Informação e Comunicação no Brasil e utilizados por organizações públicas e privadas. Desta forma, os riscos de descontinuidade desse produto no mercado parecem ser mínimos.

10.3.3. O FORNECEDOR deverá realizar a transferência de conhecimento nas versões dos softwares que serão adquiridos pelo Contratante e com isso, repassar informações de configuração, testes, procedimentos de contingência e demais informações necessárias para a operação e manutenção da solução.

10.3.4. Não se aplica o requisito pertinente aos direitos de propriedade intelectual e autoral da STIC, uma vez que não será produzido nenhum artefato, tampouco trata de desenvolvimento de software.

CLÁUSULA DÉCIMA PRIMEIRA – DA DINÂMICA DE EXECUÇÃO:

11.1. A tabela abaixo sintetiza as etapas de execução desta contratação. O prazo em todas as etapas tem como referência inicial o fim da etapa anterior.

Etapa	Descrição	Quando ocorre
1	Recebimento do pedido de fornecimento.	O TJTO encaminhará o pedido de fornecimento a qualquer tempo dentro da vigência da Ata de Registro de Preços e após a assinatura do contrato.
2	Entrega das licenças.	O prazo será de até 20 (vinte) dias úteis, contados a partir da data de assinatura do contrato ou recebimento da nota de empenho.
3	Recebimento provisório das licenças.	Imediatamente após o recebimento das licenças, para efeito de posterior verificação da conformidade do material com a especificação, nos termos do artigo 73, da Lei nº 8.666, de 1993.
4	Avaliação das licenças entregues.	Após a entrega, será realizada uma avaliação e homologação pelos responsáveis técnicos. A análise para comprovação das características técnicas consistirá em avaliar as documentações apresentadas e também informações de registro das licenças no site oficial do fabricante.

5	Recebimento Definitivo das licenças.	O responsável técnico deverá, após a comprovação do atendimento das especificações técnicas, emitir e assinar em, no máximo, 15 (quinze) dias úteis, contados do primeiro dia útil posterior à entrega dos equipamentos, o Termo de Recebimento Definitivo, nos termos do artigo 73, da Lei nº 8.666, de 1993.
6	Início da contagem do prazo de garantia.	Data da emissão do recebimento definitivo das licenças. Se for o caso de licenças vincendas, a garantia iniciará no dia subsequente após o fim da vigência desta.
7	Fim do prazo de garantia	Após 36 (trinta e seis) meses.

CLÁUSULA DÉCIMA SEGUNDA - RECEBIMENTO:

12.1. O ÓRGÃO GERENCIADOR expedirá "Termo de Recebimento Provisório", o qual deverá ser assinado pelo gestor, no prazo de 10 (dez) dias úteis, para efeito de posterior verificação da conformidade dos objetos com as especificações constantes neste Termo de Referência, nos termos do artigo 73, II, *"a"*, da Lei nº 8.666, de 1993.

12.2. Após a verificação da qualidade e quantidade dos objetos e consequente aceitação, nos termos do artigo 73, II, *"b"*, da Lei nº 8.666, 1993, o ÓRGÃO GERENCIADOR emitirá "Termo de Recebimento Definitivo", no prazo de 10 (dez) dias úteis, o qual deverá ser assinado pelo gestor.

12.3. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança dos objetos fornecidos, nem ético-profissional, para perfeita execução do objeto, dentro dos limites estabelecidos pela lei ou pelo contrato.

12.4. O FORNECEDOR é obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

CLÁUSULA DÉCIMA TERCEIRA – DO PAGAMENTO:

13.1. O FORNECEDOR deverá, obrigatoriamente, apresentar nota fiscal correspondente aos objetos fornecidos.

13.2. Os pagamentos serão efetuados após análise da conformidade dos objetos entregues discriminado na respectiva nota fiscal e o atesto do gestor do contrato.

13.3. O atesto do gestor do contrato na nota fiscal é condição indispensável para o pagamento:

13.3.1. Na ausência do gestor do contrato (férias, licença ou em viagem por interesse do ÓRGÃO GERENCIADOR), o atesto será dado pelo gestor substituto.

13.4. O ÓRGÃO GERENCIADOR reserva-se o direito de não atestar a nota fiscal para o pagamento, se os dados constantes desta estiverem em desacordo com os dados do FORNECEDOR ou, ainda, se os objetos fornecidos não estiverem em conformidade com as especificações apresentadas neste Instrumento e no Termo de Referência, ficando o pagamento suspenso até a regularização.

13.5. O pagamento será efetuado em até 30 (trinta) dias corridos, após o protocolo de recebimento da nota fiscal (momento em que o credor está adimplente com a obrigação firmada perante o ÓRGÃO GERENCIADOR), sendo que, recaindo sobre dias não úteis, o termo final será prorrogado para o dia útil

subsequente.

13.6. O pagamento será realizado, no prazo previsto no item anterior, por meio de ordem bancária em conta corrente do FORNECEDOR, quando mantidas as mesmas condições iniciais de habilitação e caso não haja fato impeditivo para o qual não tenha concorrido.

13.7. O CNPJ constante da Nota Fiscal deverá ser o mesmo indicado na proposta e nota de empenho e vinculado à conta-corrente.

13.8. O ÓRGÃO GERENCIADOR somente pagará o FORNECEDOR o que for solicitado e entregue.

13.9. Ocorrendo atraso no pagamento, e desde que tal não tenha concorrido de alguma forma o FORNECEDOR, haverá incidência de atualização monetária sobre o valor devido, pela variação acumulada do índice Geral de Preços – Disponibilidade Interna (IGP-DI), coluna 2, publicado pela FGV, ocorrida entre a data final prevista para o pagamento e a data de sua efetiva realização.

13.10. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que o FORNECEDOR providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o ÓRGÃO GERENCIADOR.

13.11. Todos os atos inerentes ao presente processo obedecerão às regras concernentes ao Sistema de Eletrônico de Informações - SEI, do ÓRGÃO GERENCIADOR.

CLÁUSULA DÉCIMA QUARTA – DAS OBRIGAÇÕES DO ÓRGÃO GERENCIADOR:

14.1. O ÓRGÃO GERENCIADOR obriga-se a:

14.1.1. Observar as leis, decretos, regulamentos, portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto do Sistema de Registro de Preços;

14.1.2. Responsabilizar-se pela lavratura do respectivo contrato ou instrumento equivalente, com base nas disposições da Lei n°. 8.666/93 e suas alterações;

14.1.3. Receber os objetos de acordo com as disposições desta Ata e do Termo de Referência;

14.1.4. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

14.1.5. Comunicar ao FORNECEDOR, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

14.1.6. Acompanhar e fiscalizar o cumprimento das obrigações do FORNECEDOR, por meio de comissão/servidor especialmente designado;

14.1.7. Prestar quaisquer esclarecimentos que venham ser formalmente solicitados pelo FORNECEDOR e pertinente ao objeto desta Ata;

14.1.8. Zelar pelo bom andamento deste Registro de Preços dirimindo quaisquer dúvidas que porventura existam;

14.1.9. Assegurar os recursos orçamentários e financeiros para custear as aquisições decorrentes desta Ata;

14.1.10. Processar e liquidar a fatura correspondente, por meio de Ordem Bancária, desde que não haja fato impeditivo imputado ao FORNECEDOR;

14.1.11. Zelar para que durante a vigência desta Ata, bem como dos contratos firmados, que sejam cumpridas as obrigações assumidas por parte do FORNECEDOR, bem como sejam mantidas todas as condições de habilitação e qualificação exigida;

14.1.12. Gerenciar, a presente Ata indicando sempre que solicitado, o nome do FORNECEDOR, o preço registrado, os quantitativos disponíveis e as especificações dos objetos registrados, observada a ordem de classificação indicada na licitação;

14.1.13. Conduzir eventuais procedimentos administrativos de renegociação de preços registrados, para fins de adequação às novas condições de mercado, e de aplicação de penalidades.

CLÁUSULA DÉCIMA QUINTA – DAS OBRIGAÇÕES DO FORNECEDOR:

15.1. O FORNECEDOR obriga-se a:

15.1.1. Observar as leis, decretos, regulamentos, portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto do Sistema de Registro de Preços;

15.1.2. Cumprir todas as obrigações constantes neste Instrumento, no Edital, seus Anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução deste Registro de Preços;

15.1.3. Atender prontamente às solicitações do ÓRGÃO GERENCIADOR no fornecimento do objeto nas quantidades e especificações deste Termo de Referência, de acordo com a necessidade desta Corte, a partir da solicitação do gestor do contrato.

15.1.4. Responsabilizar-se por todos os recursos e insumos necessários ao perfeito cumprimento do objeto contratado, devendo estar incluídas no preço proposto todas as despesas com materiais, insumos, seguros, impostos, taxas, encargos e demais despesas necessárias à perfeita execução do objeto.

15.1.5. Indicar, formalmente, preposto apto a representá-la junto ao ÓRGÃO GERENCIADOR, que deverá responder pela fiel execução do contrato.

15.1.6. Prestar todos os esclarecimentos técnicos que lhe forem solicitados pelo Contratante, relacionados com as características e funcionamento do objeto, inclusive em relação aos problemas detectados.

15.1.7. Comunicar, imediatamente, por escrito qualquer anormalidade, prestando ao Contratante os esclarecimentos julgados necessários.

15.1.8. Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados; treinados e qualificados para prestação dos serviços.

15.1.9. Manter ficha de controle do serviço, na qual serão relatadas todas as ocorrências.

15.1.10. Assumir inteira responsabilidade técnica e operacional, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas na prestação do objeto.

15.1.11. Ficar obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nas aquisições até 25% (vinte e cinco por cento) do valor inicial deste Termo de Referência, nos termos da Lei.

15.1.12. Não transferir a outrem, no todo ou em parte, o objeto desta prestação.

15.1.13. Identificar qualquer equipamento de sua posse que venha a ser utilizado nas dependências do CONTRATANTE, afixando placas de controle patrimonial, selos de segurança etc.

15.1.14. Reparar quaisquer danos diretamente causados ao ÓRGÃO GERENCIADOR ou a terceiros, por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da presente relação contratual, não excluindo ou reduzindo essa responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pelo Contratante.

15.1.15. Cumprir integralmente as exigências do Acordo de Nível de Serviço, disposto no "ANEXO C" do Termo de Referência.

15.1.16. Manter sigilo sobre todo e qualquer assunto de interesse do ÓRGÃO GERENCIADOR ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa.

15.1.17. Manter, durante a vigência desta Ata e execução dos contratos firmados, todas as condições de habilitação e qualificação exigidas na licitação, em conformidade com art. 55, inciso XIII, da Lei nº 8.666/93, incluindo a atualização de documentos de controle da arrecadação de tributos e contribuições federais e outras legalmente exigíveis.

CLÁUSULA DÉCIMA SEXTA – DA GESTÃO E FISCALIZAÇÃO:

16.1. Profissionais do FORNECEDOR: equipe composta por técnicos do FORNECEDOR, responsáveis pela execução e acompanhamento do objeto.

16.1.1. Técnico: funcionário do FORNECEDOR, responsável pela execução técnica-operacional.

16.1.2. Preposto: funcionário representante do FORNECEDOR, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

16.2. Equipe de Gestão do Contrato: equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares.

16.2.1. Gestor do Contrato: servidor responsável pela gestão contratual, conforme Decreto Judiciário nº 291, de 2009 e Portaria nº 255, de 2009, do Tribunal de Justiça do Estado do Tocantins.

16.2.2. Fiscal Demandante: servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos funcionais da solução.

16.2.3. Fiscal Técnico: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.

16.2.4. Fiscal Administrativo: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

16.3. A atuação ou a eventual omissão da Fiscalização durante a realização dos trabalhos, não poderá ser invocada para eximir o FORNECEDOR da responsabilidade no fornecimento dos produtos.

16.4. A fiscalização será sob o aspecto qualitativo e quantitativo, devendo ser anotado, em registro próprio as falhas detectadas, e comunicadas ao gestor do contrato todas as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte da Contratada.

16.5. A comunicação entre a fiscalização e o FORNECEDOR será realizada por meio de correspondência oficial e anotações ou registros no mesmo processo que tratam da aquisição dos objetos.

16.6. Quando houver necessidade o gestor deverá emitir notificações para o FORNECEDOR.

CLÁUSULA DÉCIMA SÉTIMA – DAS SANÇÕES ADMINISTRATIVAS:

17.1. O FORNECEDOR que, convocado dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar a documentação exigida ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedida de licitar e contratar com a Administração Pública do Estado do Tocantins e será descredenciada no Sistema de Cadastramento Unificado de Fornecedores (Sicaf), pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais.

17.2. Subsidiariamente, nos termos do art. 87 da Lei n°. 8.666/93, pela inexecução total ou parcial das condições estabelecidas neste Instrumento, o ÓRGÃO GERENCIADOR poderá, garantida a prévia defesa do FORNECEDOR, que deverá ser apresentada no prazo de 5 (cinco) dias úteis a contar da sua notificação, aplicar, sem prejuízo das responsabilidades penal e civil, as seguintes sanções:

a) Advertência, por escrito, quando o FORNECEDOR deixar de atender quaisquer indicações aqui constantes

b) Multa compensatória/indenizatória no percentual de 5% (cinco por cento) calculado sobre o valor contratado;

c) Suspensão temporária de participação em licitação e impedimento de contratar com o Poder Judiciário do Estado do Tocantins, pelo prazo de até 2 (dois) anos; e

d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o FORNECEDOR ressarcir o ÓRGÃO GERENCIADOR pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

17.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pelo FORNECEDOR, a este será aplicado multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor do contrato, por dia de atraso, limitada a 10% (dez por cento) do valor inadimplido.

17.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhido ao Fundo Especial de Modernização e Aprimoramento do Poder Judiciário – Funjuris, dentro do prazo de 5 (cinco) dias úteis após a respectiva notificação;

17.5. Caso não seja paga no prazo previsto no subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado pelo ÓRGÃO GERENCIADOR ou cobrada judicialmente.

17.6. Além das penalidades citadas, o FORNECEDOR ficará sujeito, ainda, no que couber, às demais penalidades referidas no Capítulo IV da Lei n°. 8.666/93.

A presente Ata, após lida e achada conforme, é assinada pelos representantes legais do ÓRGÃO GERENCIADOR e do FORNECEDOR, por meio de assinatura eletrônica, utilizando-se do Sistema Eletrônico de Informações - SEI.

Documento assinado eletronicamente por **Dennis Fernandes de Medeiros**, **Usuário Externo**, em 10/08/2021, às 09:29, conforme art. 1°, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Desembargador João Rigo Guimarães**, **Presidente**, em 12/08/2021, às 16:56, conforme art. 1°, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **3843127** e o código CRC **38715B15**.

PODER JUDICIÁRIO

TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS

Palácio da Justiça Rio Tocantins, Praça dos Girassóis, sn - Bairro Centro - CEP 77001002 - Palmas - TO - http://www.tjto.jus.br
Tribunal de Justiça

Edital Nº 198 / 2021 - PRESIDÊNCIA/DIGER/DIADM/COLIC

Tribunal de Justiça do Estado do Tocantins

Comissão Permanente de Licitação

PREGÃO ELETRÔNICO Nº 039/2021 – SRP

Regido pelas Leis n. 10.520/2002, e 12.846/2013, pela Lei Complementar n. 123/2006, pelos Decretos n. 10.024/2019, 7.892/2013 e 8.538/2015, subsidiariamente, pela Lei n. 8.666/1993. Aplica-se a esta licitação o disposto na Resolução do CNJ n.º 229, de 22 de junho de 2016.

Objeto: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA RENOVAÇÃO E AQUISIÇÃO DE LICENÇAS DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS, INCLUINDO ATUALIZAÇÕES E SUPORTE TÉCNICO PELO PERÍODO DE 36 (TRINTA E SEIS) MESES.

ABERTURA DA SESSÃO PÚBLICA:

Dia 15 de julho de 2021, às 14:00 h (horário de Brasília)

Valor Total Estimado: R$ 398.771,50 (Trezentos e noventa e oito mil setecentos e setenta e um reais e cinquenta centavos)

AMPLA CONCORRÊNCIA NO ITEM 01

EXCLUSIVA PARA ME/EPP NO ITEM 02

A participação neste pregão eletrônico ocorrerá exclusivamente por meio do sistema eletrônico (Comprasnet) e digitação da senha privativa da licitante e subsequente preenchimento da proposta de preços e encaminhamento da documentação exigida no presente edital, o qual poderá ser realizado a partir da liberação do Edital no Comprasnet até o horário de abertura da sessão pública a qual será realizada no seguinte endereço eletrônico: **https://www.gov.br/compras/pt-br/**

Orientações às licitantes: O Tribunal de Justiça do Estado do Tocantins orienta aos licitantes que analisem cuidadosamente o inteiro teor deste edital e dos respectivos anexos, antes da apresentação de suas propostas. Devendo compreender os termos da presente licitação e certificar-se de que dispõe dos recursos materiais e humanos necessários para participar da Sessão Pública e de que toda a documentação exigida está atualizada, de acordo com exigências editalícias e legais, assim como pronta para ser exibida se esta for requisitada pelo pregoeiro.

Modo de Disputa: ABERTA

Vistoria: ( ) SIM (X) NÃO

Amostra: ( ) SIM (X) NÃO

Atestado de Capacidade Técnica: (X) SIM ( ) NÃO *(Obs.: A Instrução Normativa nº 9/2018, DJ nº 4312, pág. 64/65, de 23.07.2018)*

Forma de Adjudicação: POR ITEM

Prazo para Envio da Documentação: Até 2 (duas) horas após solicitação do pregoeiro

Pedido de Esclarecimento e Impugnações: Até dia 12 de julho de 2021, até as 18:00 hs para o endereço cpl@tjto.jus.b

Pregoeiro e Equipe de Apoio: Comissão Permanente de Licitação - CPL-TJ/TO, localizada no Anexo I do Tribunal de Justiça do Estado do Tocantins (Edifício Amaro Empresarial), situado na Quadra 103 Norte, Rua NO-11, Lote 2, 7º Andar, Plano Diretor Norte, Palmas/TO, CEP 77.001-036, Telefone: (63) 3218-4590 e e-mail:cpl@tjto.jus.br.

**As sessões públicas dos pregões eletrônicos realizados por esta Corte de Justiça poderão ser acompanhados pelo endereço www.comprasgovernamentais.gov.br, selecionando as opções Consultas > Pregões > Em andamento > Cód. UASG "925814". O edital e outros anexos estão disponíveis para download no Sistema Comprasnet e podem ser baixados acessando o link:*http://www.tjto.jus.br/index.php/cidadao/licitacoes

PREGÃO ELETRÔNICO N.º 039/2021 - SRP

PREÂMBULO

O TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS, UASG 925814, torna público aos interessados, através de sua equipe de **Pregoeiros** designados pela Portaria nº 161, de 05 de fevereiro de 2020, que realizará licitação para **REGISTRO DE PREÇOS**, na modalidade **PREGÃO** em sua forma **ELETRÔNICO**, cujo critério de julgamento será o de **MENOR PREÇO POR ITEM**, autorizada nos autos nº **21.0.000002638-4**, visando a **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA RENOVAÇÃO E AQUISIÇÃO DE LICENÇAS DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS, INCLUINDO ATUALIZAÇÕES E SUPORTE TÉCNICO PELO PERÍODO DE 36 (TRINTA E SEIS) MESES.** A sessão pública será realizada no **dia 15 de julho de 2021, às 14:00 h (horário de Brasília)**, na sala da Comissão de Licitação, localizada no Anexo I do Tribunal de Justiça do Estado do Tocantins (Edifício Amaro Empresarial), situado na Quadra 103 Norte, Rua NO-11, Lote 2, 7º Andar, Plano Diretor Norte, Palmas/TO, por meio do sítio **www.gov.br/compras/pt-br/.** A presente licitação será regida pelas Leis n. 10.520/2002, 12.846/2013, pela Lei Complementar n. 123/2006, pelos Decretos n. 10.024/2019, 7.892/2013 e 8.538/2015, pelas condições constantes neste Edital e subsidiariamente, pela Lei n. 8.666/1993. Aplica-se a esta licitação o disposto na Resolução do CNJ n.º 229, de 22 de junho e 2016.

Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça à abertura do certame na data e horário marcado, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e local estabelecidos no preâmbulo deste edital, desde que não haja comunicação do Pregoeiro em contrário.

1 – DO OBJETO

1.1. A presente licitação tem como objeto o **Registro de Preços** visando futura **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA RENOVAÇÃO E AQUISIÇÃO DE LICENÇAS DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS, INCLUINDO ATUALIZAÇÕES E SUPORTE TÉCNICO PELO PERÍODO DE 36 (TRINTA E SEIS) MESES**, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será dividida em 02 itens, conforme tabela constante no subitem 1.1 do Termo de Referência (Anexo I).

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

2 - DA DOTAÇÃO ORÇAMENTÁRIA

2.1. A despesa com a execução do objeto desta licitação correrá à conta da Dotação Orçamentária com valor de referencia **R$ 398.771,50 (Trezentos e noventa e oito mil setecentos e setenta e um reais e cinquenta centavos)** e será consignado:

Unidade Gestora: 050100 - Tribunal de Justiça

Classificação Orçamentária - PI: 0501.02.126.1145.2249

Natureza de Despesa: 33.90.40

Fonte de Recursos: 0100

e/ou

Unidade Gestora: 060100 - FUNJURIS

Classificação Orçamentária - PI: 0601.02.126.1145.4231

Natureza de Despesa: 33.90.40

Fonte de Recursos: 0240

3 - DAS CONDIÇÕES PARA PARTICIPAÇÃO

3.1. Poderão participar deste pregão eletrônico, interessados **desde que:**

a) atendam às condições deste Edital e seus Anexos, inclusive quanto à documentação, e estejam devidamente credenciadas na Secretaria de Logística e Tecnologia da Informação (SLTI), do Ministério do Planejamento, Desenvolvimento e Gestão, por meio do sítio www.comprasgovernamentais.gov.br, para acesso ao sistema eletrônico;

b) possuam registro cadastral atualizado no Sistema de Cadastramento Unificado de Fornecedores (SICAF). Esse registro também será requisito obrigatório para fins de habilitação.

3.2. Para o cumprimento do disposto no art. 47 da Lei Complementar nº 123/2006, o qual estabelece o tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte ficam estabelecidos os seguintes critérios de participação, onde:

3.2.1. O item 01 é de ampla concorrência a todas as empresas do ramo pertinente ao objeto licitado neste certame;

3.2.2. O item 02 é exclusivo para participação de ME/EPP do ramo pertinente ao objeto licitado neste certame;

3.3. Para fins desta licitação, considera-se microempresa e empresa de pequeno porte o agricultor familiar, o produtor rural pessoa física e o microempreendedor individual, nos termos do art. 1º do Decreto n. 8.538/2015.

3.4. Aplicam-se a Lei Complementar n. 123/2006 e o Decreto n. 8.538/2015, somente para microempresas, empresas de pequeno porte ou sociedades cooperativas que se enquadram na condição estabelecida no art. 34 da Lei n. 11.488/2007.

3.4.1. As microempresas, as empresas de pequeno porte ou sociedades cooperativas, que se enquadram na condição estabelecida no art. 34 da Lei n. 11.488/2007, que desejarem fazer jus aos benefícios previstos na Lei Complementar n. 123/2006 deverão manifestar, em campo próprio, sob as penas da lei, declaração de que atendem aos requisitos do art. 3º da referida Lei.

3.5. A Secretaria de Logística e Tecnologia da Informação-SLTI, do Ministério do Planejamento, Desenvolvimento e Gestão atuará como órgão provedor do sistema eletrônico Comprasnet.

3.5.1. Os licitantes deverão utilizar o certificado digital para acesso ao Sistema Eletrônico, por meio do sítio www.comprasgovernamentais.gov.br, onde também deverão informar-se a respeito do seu funcionamento e regulamento e buscar instruções detalhadas para sua correta utilização.

3.5.2. O uso da senha de acesso pela licitante é de sua exclusiva responsabilidade, incluindo qualquer transação por ele efetuada diretamente, ou por seu representante, não cabendo ao provedor do sistema ou ao Tribunal de Justiça do Estado do Tocantins responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

3.6. Como requisito para participação no pregão eletrônico, a licitante deverá declarar, em campo próprio do sistema, o pleno conhecimento do edital, o cumprimento dos requisitos para a habilitação e a conformidade de sua proposta com as exigências do presente Edital.

3.7. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e da proposta de preços sujeitará a licitante às sanções previstas na legislação e no presente Edital.

3.8. Não poderão participar desta licitação:

a) Nos itens de participação exclusiva para ME/EPP, empresas que não se enquadrem na condição de microempresas, empresas de pequeno porte ou sociedades cooperativas enquadradas na condição estabelecida no art. 34 da Lei 11.488/2007;

b) **pessoas jurídicas que não explorem atividade compatível com o objeto desta licitação;**

c) que tenham sido declarados inidôneos para licitar ou contratar com a Administração Pública;

d) punidas com suspensão do direito de licitar e contratar com o Tribunal de Justiça do Estado do Tocantins;

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

f) que estejam sob falência, concurso de credores, concordata ou em processo de dissolução ou liquidação;

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

h) consórcio de empresas, qualquer que seja sua forma de constituição.

i) entidades empresariais que estejam reunidas em consórcio; **exceto**, aos consórcios formados exclusivamente por microempresas e empresas de pequeno porte, desde que a soma das receitas brutas anuais não ultrapassem o limite previsto no inciso II do **caput** do art. 3º da Lei Complementar nº 123, de 2006.

3.9. Os documentos apresentados nesta licitação deverão conter os números de CNPJ dos estabelecimentos que, a critério de uma mesma pessoa jurídica licitante, serão responsáveis pela execução do objeto e que poderão emitir, em decorrência, ao longo da vigência do contrato, as notas fiscais que serão apresentadas a pagamento.

3.10. Quando a certidão for emitida com prazo de validade indeterminado e/ou o prazo de validade da certidão não estiver expresso em seu instrumento, aquela expedida nos últimos 60 (sessenta) dias que antecederem à data da sessão deste certame será considerada válida, exceto quando houver norma (lei, resolução, instrução normativa, portaria etc.) estabelecendo prazo de validade inferior, hipótese na qual prevalecerá o prazo nela previsto. Os prazos aqui referidos serão contados a partir da data de emissão, inclusive.

4 - DO CREDENCIAMENTO

4.1. A licitante deverá credenciar-se no sistema "Pregão Eletrônico", no sítio www.comprasgovernamentais.gov.br, observado o seguinte:

a) o credenciamento far-se-á mediante atribuição de chave de identificação e de senha, pessoal e intransferível, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil, para acesso ao sistema eletrônico;

b) a licitante deve comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a inviabilidade do uso da senha, para imediato bloqueio de acesso;

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

4.2. 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 por ele praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do Tribunal de Justiça do Estado do Tocantins por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

4.3. A licitante responsabilizar-se-á por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas, assim como os lances inseridos durante a sessão pública.

4.4. 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.

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

5 - DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Divulgado o Edital no endereço eletrônico, as licitantes encaminharão, exclusivamente por meio do sistema, mediante digitação de senha privativa, a proposta com a descrição do objeto ofertado e o preço, formulada de acordo com o Anexo I, e os documentos de habilitação exigidos neste edital, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas e dos documentos de habilitação.

5.2. Ao lançar a proposta de preços no sistema eletrônico, a licitante deverá incluir o detalhamento do objeto ofertado no campo "Descrição Detalhada do Objeto". Caso o número de caracteres seja insuficiente, deverá incluir descrição resumida contendo as informações essenciais.

5.2.1. Até a abertura da sessão pública, a licitante poderá retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

5.2.2. Os valores ofertados deverão ser calculados com duas casas decimais.

5.3. A licitante deverá consignar em campo adequado do sistema eletrônico o valor unitário de cada item e, se for o caso, de cada item que compõe o grupo, já considerados e inclusos os tributos, fretes, tarifas e demais despesas decorrentes da execução do objeto.

5.4. Não será aceita oferta de objeto com especificações diferentes das indicadas nos anexos deste Edital.

5.4.1. Em caso de divergência entre as especificações técnicas descritas no Sistema Comprasnet e as descritas neste Edital, prevalecerão estas.

5.5. No caso de sistema de registro de preços quando a proposta do licitante vencedor não atender ao quantitativo total estimado para a contratação, poderá ser convocada a quantidade de licitantes necessária para alcançar o total estimado, respeitada a ordem de classificação, observado o preço da proposta vencedora, precedida de posterior habilitação, nos termos do disposto no Decreto 10.024/2019.

5.6. As Microempresas e Empresas de Pequeno Porte **DEVERÃO** encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1° da LC n° 123, de 2006.

5.7. Na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, não haverá ordem de classificação das propostas, o que ocorrerá somente quando findar a realização dos procedimentos de negociação e julgamento da proposta.

5.8. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados pelo sistema para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

5.9. Para garantir a integridade da documentação e da proposta, recomenda-se que contenham índice, folhas numeradas, com o nome, logotipo ou logomarca da licitante.

5.10. A **proposta de preços deverá** ser redigida em língua portuguesa, sem alternativas, opções, emendas, ressalvas, borrões, rasuras ou entrelinhas, e dela deverá constar:

a) **número do Pregão Eletrônico, identificação social, número do CNPJ** responsável pela execução do objeto, assinatura do representante legal da proponente, **número de telefone, endereço, dados bancários, e indicação de endereço eletrônico (e-mail);**

b) indicação do responsável pela assinatura da Ata de Registro de Preços, com o número da carteira de identidade, CPF, e, caso não seja sócio da empresa, procuração passada em instrumento público ou particular, com poderes para assinatura do instrumento, em nome da proponente;

c) prazo de validade da proposta de 60 (sessenta) dias, a contar da data de abertura da sessão pública estabelecida no preâmbulo deste Edital;

d) indicação de preço em real, com indicação do **valor unitário e total do item**, se for o caso, em algarismos e por extenso, calculados com duas casas decimais;

e) **descrição clara e detalhada do produto/serviço ofertado, em conformidade com as especificações técnicas constantes no Termo de Referência (Anexo I do Edital), de forma a viabilizar a análise de sua conformidade, com indicação do fabricante/marca/modelo, datasheet do produto, se for o caso, além da indicação do site do fabricante, de quantidade, prazo de entrega, de garantia e demais características dos produtos/serviços, no que for aplicável;**

5.10.1. Para fins de análise técnica do objeto ofertado na proposta e sua conformidade às especificações do instrumento convocatório, será colhida manifestação do setor demandante da aquisição/contratação ou da área técnica especializada no objeto.

5.10.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada e implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o disposto no instrumento convocatório, assumindo a licitante o compromisso pela adequada execução do objeto.

5.10.3. Os preços de referência estabelecidos pela Administração no Mapa de Preços devem ser observados pelo licitante, pois serão considerados os preços máximos a serem contratados pelo item e/ou grupo de itens, se for o caso.

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

5.11. Os **documentos para habilitação**, relativos ao estabelecimento responsável pela execução do objeto, serão:

Habilitação jurídica

a) **registro comercial**, no caso de empresário individual, acompanhando das respectivas alterações, se houver; Em se tratando de microempreendedor individual – MEI: **Certificado da Condição de Microempreendedor Individual - CCMEI**, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

b) **ato constitutivo, estatuto ou contrato social em vigor**, devidamente **registrado na Junta Comercial** da respectiva sede, **acompanhado de documento comprobatório de seus administradores** assim como das respectivas **alterações ou da consolidação** respectiva, se houver; e em se tratando de sociedades comerciais por ações, acompanhado de documentos de eleição de seus administradores e alterações ou da consolidação respectiva;

Regularidade fiscal e trabalhista

c) prova de regularidade relativa à Seguridade Social;

d) Certificado de Regularidade do FGTS – CRF, emitido pela Caixa Econômica Federal;

e) prova de regularidade para com a Fazenda Federal;

f) prova de regularidade para com a Fazenda Estadual;

g) prova de regularidade para com a Fazenda Municipal da sede da licitante;

h) Certidão Negativa de Débitos Trabalhistas – CNDT, emitida pela Justiça do Trabalho;

Qualificação econômico-financeira

i) **Balanço patrimonial e demonstrações contábeis** do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancete ou balanços provisórios.

i.1. No caso de empresa constituída neste exercício financeiro, a exigência da alínea anterior, será atendida mediante a apresentação de balanço de abertura.

i.2. É admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

i.3. Comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG) e Liquidez Corrente (LC), iguais ou superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

LG =	Ativo Circulante + Realizável a Longo Prazo
	Passivo Circulante + Passivo Não Circulante

LC =	Ativo Circulante
	Passivo Circulante

i.4. As empresas que apresentarem resultado inferior a 1(um) em qualquer dos índices de Liquidez Geral (LG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor total estimado da contratação ou do grupo pertinente.

j) **Certidão Negativa de Falência ou Concordata** ou, se for o caso, Certidão de Recuperação Judicial, expedida pelo Cartório Distribuidor da sede da pessoa jurídica;

j.1) No caso de certidão positiva de recuperação judicial ou extrajudicial, o licitante deverá apresentar a comprovação de que o respectivo plano de recuperação foi acolhido judicialmente, na forma do art. 58, da Lei n.º 11.101, de 09 de fevereiro de 2005, sob pena de inabilitação, devendo, ainda, comprovar todos os demais requisitos de habilitação.

Declarações exigidas

k) Declaração, em campo próprio no sistema eletrônico, de cumprimento do disposto no art. 7º, XXXIII, da Constituição Federal/1988 (trabalho de menores de idade, observada a Lei n. 9.854/1999);

l) Declaração, em campo próprio no sistema eletrônico, de inexistência de fato superveniente impeditivo da habilitação;

m) Declaração, em campo próprio no sistema eletrônico, de elaboração independente de proposta.

Qualificação Técnica

l) Atestado de capacidade técnica emitido por pessoa jurídica de direito público ou privado, com a finalidade de comprovar que o licitante forneceu objetos e/ou prestou serviços satisfatoriamente, em características compatíveis com o objeto da licitação, nos termos da Instrução Normativa Nº 9, de 20 de julho de 2018, do Tribunal de Justiça do Estado do Tocantins, de 20 de julho de 2018, (DJ nº 4312, de 23.07.2018), a qual dispõe que:

l.1) O atestado de Capacidade Técnica tem a finalidade de comprovar que o licitante forneceu ou está fornecendo objetos e/ou prestou ou está prestando serviços satisfatoriamente, de forma compatível com o objeto da contratação.

l.2) O atestado emitido por pessoa jurídica de direito privado será assinado pelo representante legal da pessoa emitente, o qual se responsabilizará na forma da lei.

l.3) O atestado deverá constar, no mínimo, os seguintes dados do emitente: razão social e dados para contato; e do favorecido: razão social, número do CNPJ, objeto do contrato e dados para contato.

l.4) Será admitida a somatória de atestados de capacidade técnica sempre que inexistir motivo para a exigência de atestado único, independente da época de expedição ou localidade.

5.12. As declarações e ou relatórios extraídos do Sistema de Cadastramento Unificado de Fornecedores – SICAF substituirão os documentos relacionados nas alíneas 'a', 'b', 'c', 'd', 'e', 'f', 'g, 'h' e 'i' do item 5.11, para fins de habilitação da licitante cadastrada naquele sistema, desde que:

a) as informações relativas àqueles documentos estiverem disponíveis para consulta na data da sessão de recebimento da proposta e da documentação; e

b) se estiverem dentro dos respectivos prazos de validade.

c) desde que assegure aos demais licitantes o direito de acesso aos dados constantes ou extraídos do sistema.

5.13. Caso nos registros cadastrais conste algum documento com prazo de validade vencido, a licitante deverá encaminhar comprovante idêntico, com o respectivo prazo atualizado, dentro do prazo e condições estabelecidas no item 7.3, sob pena de inabilitação.

5.14. As microempresas, empresas de pequeno porte e as sociedades cooperativas (desde que se enquadrem na condição estabelecida no art. 34 da Lei n. 11.488/2007) deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição.

5.14.1. Havendo alguma restrição na comprovação da regularidade fiscal das microempresas, empresas de pequeno porte ou sociedades cooperativas (somente as que se enquadram na condição estabelecida no art. 34 da Lei n. 11.488/2007), será assegurado o prazo de 5 (cinco) dias úteis, prorrogáveis por igual período, a critério do pregoeiro, a contar do momento em que se declarar o vencedor do certame, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

5.14.2. A não regularização da documentação implicará decadência do direito à contratação, sem prejuízo das sanções previstas em lei.

5.15. Se a documentação de habilitação não estiver completa e correta ou contrariar qualquer dispositivo deste Edital e seus Anexos, o Pregoeiro considerará o licitante inabilitado, sendo convocado outro licitante, observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções legais cabíveis.

5.16. Será inabilitado a licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, apresentá-los em desacordo com o estabelecido neste Edital, ou não atender a convocação do pregoeiro.

5.17. As certidões que não declararem expressamente o período de validade, para fins desta licitação, deverão ter sido emitidas nos 60 (sessenta) dias imediatamente anteriores à data prevista para a abertura da sessão, sendo os prazos aqui referidos contados a partir da data de emissão, inclusive.

5.18. No caso de empresas estrangeiras participantes da licitação, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados com tradução livre. Sendo declarada vencedora do certame, os documentos de habilitação deverão ser traduzidos por tradutor juramentado no País e apostilados (Apostila de Haia) como condição para assinatura do contrato ou da ata de registro de preços.

5.19. É facultado ao Pregoeiro ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo.

5.20. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.21. Não serão aceitos documentos novos após a abertura da sessão pública, observados os itens 7.3 deste edital.

6 - DA ABERTURA DA SESSÃO PÚBLICA, DA CLASSIFICAÇÃO DAS PROPOSTAS E DA ETAPA COMPETITIVA DE LANCES

6.1. A abertura da presente licitação dar-se-á em sessão pública na internet, na data e horário indicados no preâmbulo deste Edital, ocasião em que o pregoeiro utilizando de sua chave de acesso e senha procederá a abertura no sítio www.comprasgovernamentais.gov.br.

6.2. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

6.3. A licitante deverá acompanhar as operações no sistema eletrônico durante a sessão pública do pregão eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

6.4. Aberta a sessão pública, o Pregoeiro verificará as propostas apresentadas, desclassificando, motivadamente, aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, com acompanhamento em tempo real pelos demais participantes.

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

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

6.5. O sistema ordenará automaticamente as propostas classificadas pelo Pregoeiro, sendo que somente estas participarão da fase competitiva de lances.

6.6. Aberta a etapa competitiva de lances, as licitantes classificadas poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informadas do recebimento e respectivo horário de registro e valor.

6.7. Na formulação de lances, as licitantes deverão observar os seguintes aspectos:

a) As licitantes poderão oferecer lances sucessivos, observados o horário fixado para abertura da sessão e as regras estabelecidas neste instrumento convocatório.

b) A licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema, observado, quando houver, o 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.

c) Não serão aceitos dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro.

d) Na etapa competitiva dos grupos, a classificação final será pelo valor total do grupo, contudo a disputa será por item, devendo a licitante ofertar lances para cada item que compõe o grupo. A cada lance ofertado, o sistema atualizará automaticamente o valor

total do grupo.

6.8. Durante a sessão pública deste pregão, as licitantes serão informadas, em tempo real, do valor do menor lance registrado, vedada a identificação do seu detentor.

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

6.10. Será adotado para o envio de lances o modo de **disputa "aberto"**, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

6.11. 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 **1% (um por cento)**.

6.12. 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 finais.

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

6.14. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

6.15. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

6.16. Na fase competitiva, o pregoeiro poderá excluir, justificadamente, lance de valor considerado inexequível.

6.17. Na hipótese de o sistema eletrônico desconectar para o pregoeiro no decorrer da fase competitiva e permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

6.18. Quando a desconexão persistir por tempo superior a **10 (dez) minutos**, a sessão pública será suspensa e reiniciada somente decorridas **24 (vinte e quatro) horas** após a comunicação do fato aos participantes, no sítio eletrônico www.comprasgovernamentais.gov.br.

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

6.19.1. Caso ocorrerá empate entre propostas iguais não seguidas de lances, o sistema eletrônico realizará um sorteio da proposta vencedora dentre as propostas empatadas.

7 – DA FASE DE NEGOCIAÇÃO, DA ACEITABILIDADE DAS PROPOSTAS E DA HABILITAÇÃO

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

7.2. A negociação será realizada por meio do sistema eletrônico e será registrada no chat, podendo ser acompanhada pelos demais licitantes.

7.3. Encerrada a etapa de negociação, o pregoeiro examinará a proposta ajustada ao menor lance quanto à adequação ao objeto e à compatibilidade de preço em relação ao máximo estipulado para contratação e verificará a habilitação do licitante nos termos exigidos neste edital.

7.4. O Pregoeiro solicitará ao licitante melhor classificado que, no prazo de **02 (duas) horas**, envie a proposta final realinhada ao último lance ofertado ou negociado, bem como para envio de documentos complementares à proposta e à habilitação, quando necessários à confirmação daqueles exigidos no Edital e já apresentados, não podendo constar documentos novos, que deveriam ter sido cadastrados juntamente com a proposta, conforme o § 3° do art. 43 da Lei n° 8.666/93.

7.4.1. O prazo estabelecido no item 7.3 poderá ser prorrogado por igual período, mediante solicitação escrita e justificada do licitante, formulada antes de findo o prazo estabelecido inicialmente, e formalmente aceita pelo pregoeiro, em atendimento ao interesse público na obtenção da melhor proposta.

7.4.2. Quando do envio da proposta ajustada, a licitante interessada poderá evidenciar informações que eventualmente tenham constado de forma implícita na proposta originária.

7.4.3. Caso necessário o Pregoeiro poderá convocar o licitante para envio de documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo e condições estabelecidas no item 7.3, sob pena de não aceitação da proposta.

7.4.3.1. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos ou folhetos, encaminhados pelo sistema eletrônico, sob pena de não aceitação da proposta.

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

7.5. Não serão considerados novos os documentos e/ou informações que possam ser obtidos mediante consulta gratuita, aberta a qualquer interessado, a bancos de dados de órgãos e/ou entidades públicos, privados e/ou de caráter público, que estejam

disponíveis na rede mundial de computadores.

7.6. Será desclassificada a proposta ou o lance vencedor que apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 -TCU - Plenário), ou que apresentar preço manifestamente com valores irrisórios ou de valor zero.

7.7. Se a proposta classificada em primeiro lugar não for aceitável ou se a licitante não atender às exigências habilitatórias, o pregoeiro examinará a subsequente e, assim, sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda aos requisitos deste Edital.

7.8. Havendo necessidade de analisar minuciosamente os documentos apresentados, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

7.9. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata.

7.10. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

7.11. O licitante que abandonar o certame, deixando de enviar a documentação solicitada, será desclassificado e sujeitar-se-á a sanções previstas neste edital.

7.12. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto nos **itens 5.11 e 5.12** neste Edital.

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

a) SICAF;

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

7.13.1. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

7.13.2. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

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

7.14.1. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

7.15. Para fins de habilitação no presente certame, os licitantes deverão atender às exigências estabelecidas no item 5.11 deste Edital.

7.16. Somente haverá a necessidade de apresentação dos documentos originais (não-digitais) quando houver dúvida em relação à integridade do documento digital.

7.16.1. **Caso solicitado pelo Pregoeiro, VIA CHAT**, os documentos de que tratam o intem 7.16 deverão ser encaminhados, no prazo de até 07 (sete) dias úteis, contados da solicitação, para Comissão Permanente de Licitação, Anexo I do Tribunal de Justiça do Estado do Tocantins, Edifício Amaro Empresarial, situado na Quadra 103 Norte, Rua NO 11, Lote 2, 7º Andar, Plano Diretor Norte, Palmas/TO, CEP 77.001-036.

7.18. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

7.19. O licitante provisoriamente vencedor em um item/grupo, que estiver concorrendo em outro item/grupo, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item/grupo em que venceu às do item/grupo em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

7.19.1. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) item(ns) de menor(es) valor(es) cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

7.20. Será declarada vencedora a licitante que, atendidas as demais exigências fixadas neste edital, apresentar o menor valor para o item ou grupo.

7.21. Constatado o atendimento às exigências de habilitatorias fixadas neste Edital, o licitante será declarado vencedor e da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

8 – DAS AMOSTRAS

8.1. Não se aplica.

9 - DOS RECURSOS

9.1. Uma vez cancelado o item ou declarado o vencedor, e decorrida a fase de regularização fiscal e trabalhista da licitante qualificada como microempresa ou empresa de pequeno porte, se for o caso, será concedido o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

9.1.1. A falta de manifestação imediata e motivada da licitante implicará decadência do direito de recurso e o pregoeiro estará autorizado a adjudicar o objeto à licitante declarada vencedora.

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

9.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

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

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

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

9.4. Os autos do processo permanecerão com vista franqueada aos interessados, para tanto a solicitação de vista deverá ser encaminhada à CPL no e-mail:cpl@tjto.jus.br.

10 – DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

10.1. Encerrada a sessão pública, sem que haja interposição de recursos, o objeto do certame será adjudicado ao licitante declarado vencedor, e em seguida, os autos serão encaminhados à autoridade competente para verificar a regularidade dos atos praticados e, se for o caso, deliberar sobre a homologação do presente certame.

10.2. Havendo interposição de recursos, o procedimento licitatório será adjudicado e homologado pela autoridade superior, após verificar a regularidade dos atos praticados e proferida a decisão quanto aos recursos interpostos.

11 - DA REABERTURA DA SESSÃO PÚBLICA

11.1. A sessão pública poderá ser reaberta:

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

11.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1° da LC n° 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

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

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

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

12 - DA GARANTIA DE EXECUÇÃO

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

13 - DA ATA DE REGISTRO DE PREÇOS

13.1. Da Ata de Registro de Preços e dos Preços Registrados

a) Homologado o resultado da licitação e respeitada a ordem de classificação, será formalizada a Ata de Registro de Preços, documento vinculativo obrigacional que, após, cumpridos os requisitos de publicidade, terá efeito de compromisso de fornecimento nas condições estabelecidas

b) Encerrado o procedimento licitatório, o vencedor será notificado pelo Tribunal de Justiça do Estado do Tocantins para, no prazo de até **5 (cinco) dias corridos** a contar do recebimento da notificação, **para assinar a Ata de Registro de Preços (Anexo II).**

c) A Ata de Registro de Preços a ser firmada terá a validade de um ano, conforme art. 15, § 3°, inciso III, da Lei nº 8.666/93.

d) A existência de preços registrados não obriga o Tribunal de Justiça do Estado do Tocantins a firmar as contratações que deles poderão advir, facultando-se a realização de licitação específica para os serviços pretendidos. Nesse caso, o beneficiário do registro de preços terá preferência de contratação, em igualdade de condições.

e) A Ata de Registro de Preços é um documento vinculativo obrigacional, com características de compromisso para a futura contratação com o fornecedor melhor classificado.

e.1) Serão registrados na Ata de Registro de Preços, nessa ordem, os preços e quantitativos do licitante mais bem classificado durante a etapa competitiva e os preços e quantitativos dos licitantes que tiverem aceito cotar seus bens ou serviços em valor igual ao do licitante mais bem classificado (cadastro de reserva), respeitada a ordem da última proposta apresentada durante a fase competitiva.

f) Após a publicação do extrato da Ata de Registro de Preços, no Diário da Justiça Eletrônico, poderão ser firmados os contratos ou documento equivalente dentro do prazo de validade do Registro;

f.1) Os preços registrados e a indicação dos respectivos fornecedores serão divulgados no Diário da Justiça Eletrônico e ficarão disponibilizados no site www.tjto.jus.br durante toda a vigência da Ata de Registro de Preços;

g) A contratação formalizar-se-á mediante instrumento particular, observadas as cláusulas e condições deste Edital, da Ata de Registro de Preços e da proposta vencedora;

h) O fornecedor deverá manter-se, durante a vigência da Ata de Registro de Preços, em compatibilidade com as condições de habilitação assumidas na licitação, renovando as respectivas certidões e encaminhando-as à Divisão de Contratos e Convênios do Tribunal de Justiça do Estado do Tocantins, no prazo máximo de 48 (quarenta e oito) horas, a partir da solicitação das mesmas;

j) Caso a licitante classificada em primeiro lugar, após convocada, se recusar a assinar a Ata de Registro de Preços ou tiver seu registro cancelado, sem prejuízo das cominações previstas neste edital, o Tribunal de Justiça do Estado do Tocantins **convocará os licitantes remanescentes, na ordem de classificação, para que seus preços sejam registrados**, atendidas as especificações e prazos constantes neste edital.

i) Caberá ao órgão aderente à Ata de Registro de Preços, verificar junto ao fornecedor a capacidade de fornecimento dos produtos, bem como consultar ao Tribunal de Justiça do Estado do Tocantins sobre a sua anuência;

i.1) Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação do fornecimento, desde que não venha a prejudicar as obrigações anteriormente assumidas;

i.2) As aquisições ou as contratações adicionais de que trata a alínea "i" não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos de cada item do instrumento convocatório e registrado na ata de registro de preços do Tribunal de Justiça do Estado do Tocantins e dos órgãos participantes;

i.2.1) O quantitativo de que trata o item i.2 não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços do Tribunal de Justiça do Estado do Tocantins e da ata de registro de preços dos órgãos participantes, independente do número de órgão não participantes que aderirem.

j) O Registro dos licitantes que aceitarem cotar os bens e serviços com preços iguais aos do licitante vencedor, obedecidos à ordem de classificação do certame, será incluído na respectiva ata de registro de preços por meio de anexo, constituindo-se em formação de cadastro de reserva.

13.2. Da Variação dos Preços Registrados

a) A revisão de preços só será admitida no caso de comprovação de desequilíbrio econômico-financeiro, por meio de planilha de custos demonstrativa da majoração e após ampla pesquisa de mercado.

a.1) Para a concessão da revisão dos preços, a empresa deverá comunicar ao Tribunal de Justiça do Estado do Tocantins a variação dos preços, por escrito e imediatamente, com pedido justificado de revisão do preço registrado, anexando documentos comprobatórios da majoração e/ou planilha de custos.

a.2) Caso o Tribunal de Justiça do Estado do Tocantins já tenha emitido a nota de empenho respectiva, para que a empresa realize o fornecimento dos produtos, e a empresa ainda não tenha solicitado a revisão de preços, esta não incidirá sobre o(s) pedido(s) já formalizado(s) e empenhado(s).

b) O Tribunal de Justiça do Estado do Tocantins terá o prazo de 30 (trinta) dias, a partir do recebimento do pleito, para análise dos pedidos de revisão recebidos.

b.1) Durante esse período a empresa deverá fornecer os produtos pelo preço registrado e no prazo ajustado, mesmo que a revisão seja julgada procedente pelo Tribunal de Justiça do Estado do Tocantins. Nesse caso, o Tribunal de Justiça do Estado do Tocantins procederá ao reforço dos valores pertinentes aos produtos empenhados após o pedido de revisão.

b.2) A empresa obrigar-se-á a realizar o fornecimento dos produtos pelo preço registrado caso o pedido de revisão seja julgado improcedente.

c) Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao preço praticado no mercado o Tribunal convocará o fornecedor visando à negociação para redução de preços e sua adequação ao praticado pelo mercado;

c.1) Frustrada a negociação, o fornecedor será liberado do compromisso assumido.

d) Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor, mediante requerimento devidamente comprovado, não puder cumprir o compromisso, o Tribunal de Justiça do Estado do Tocantins poderá liberar o fornecedor da obrigação assumida, sem aplicação da penalidade, confirmando a veracidade dos motivos e comprovantes apresentados, desde que a comunicação ocorra antes do pedido de fornecimento.

e) Em qualquer hipótese, os preços decorrentes da revisão não poderão ultrapassar os praticados no mercado, mantendo-se a diferença percentual apurado entre o valor originalmente constante da proposta do fornecedor é aquela vigente no mercado à época do registro – equação econômico-financeiro.

f) Será considerado preço de mercado o que for igual ou inferior à média daqueles apurados pelo Tribunal de Justiça do Estado do Tocantins para o objeto pesquisado.

13.3. Do Cancelamento dos Preços Registrados

13.3.1. O registro do fornecedor poderá ser cancelado, garantida a prévia defesa, no prazo de 05 (cinco) dias úteis, a contar do recebimento da notificação, nas seguintes hipóteses:

I - Pela Administração, quando:

a) o fornecedor não cumprir as exigências contidas no presente Edital ou Ata de Registro de Preços;

b) o fornecedor der causa à rescisão administrativa, da contratação decorrente do registro de preços, por um dos motivos elencados no art. 78 e seus incisos da Lei nº. 8.666/93, alterada pela Lei nº 8.883/94;

c) o fornecedor não aceitar reduzir o seu preço registrado, quando este se apresentar superior ao praticado pelo mercado;

d) por razões de interesse público, devidamente fundamentadas, na forma do inciso XII, do art. 78 da Lei nº. 8.666/93, alterada pela Lei nº. 8.883/94;

II - Pelo fornecedor, quando, mediante solicitação por escrito, comprovar estar impossibilitado de cumprir as exigências deste instrumento convocatório que deu origem ao registro de preços;

13.3.2. O cancelamento será precedido de processo administrativo, sendo que a decisão final deverá ser fundamentada;

13.3.3. A comunicação do cancelamento do registro do fornecedor será feita por escrito, juntando-se o comprovante de recebimento;

13.3.4. No caso do fornecedor encontrar-se em lugar ignorado, incerto ou inacessível, a comunicação será feita por publicação, no Diário da Justiça do Estado do Tocantins, considerando-se cancelado o registro do fornecedor, a partir do 5º dia útil, a contar da publicação; e

13.3.5. A solicitação do fornecedor para cancelamento do registro de preço, não o desobriga do fornecimento dos produtos, até a decisão final do órgão gerenciador, a qual deverá ser prolatada no prazo máximo de 30 (trinta) dias, facultada à Administração a aplicação das penalidades previstas neste instrumento convocatório, caso não aceitas as razões do pedido.

13.4. Da Formação do Cadastro de reserva

13.4.1. No ato da homologação do certame pela autoridade competente, as licitantes cujas propostas não tenham sido recusadas serão convocadas, por e-mail, para manifestarem interesse em participar do cadastro de reserva. Aquelas interessadas deverão reduzir seus preços ao valor da proposta da licitante declarada vencedora, com vistas a formação do cadastro de reserva.

13.4.1.1. A manifestação em integrar o cadastro de reserva não altera o resultado do certame, cabendo apenas aos itens com propostas adjudicadas, e caso as licitantes não se manifestem no prazo estabelecido ocorrerá a preclusão do seu direito.

13.4.1.2. O licitante que compuser o cadastro de reserva disposto no item 15.4.1, será convocado em caso de cancelamento do registro de preços do primeiro colocado, nas hipóteses previstas nos art. 20 e 21 do Decreto n.º 7.892/13.

13.4.1.3. Se mais de um licitante manifestar interesse em compor o cadastro de reserva a que se refere o item 15.4.1, os mesmos serão classificados segundo a ordem da última proposta apresentada na etapa de lances, excluídos o percentual referente à margem de preferência, quando o objeto não atender o disposto no art. 3º da Lei n.º 8.666/93.

13.4.1.4. Uma vez cancelado o registro de preços nos termos do item 15.4.1.2, a autoridade competente, convocará os participantes do certame, designando o dia e hora para realização da habilitação dos fornecedores que comporão o cadastro de reserva, observados a ordem de classificação.

13.4.2. A recusa injustificada do fornecedor classificado em assinar a ata, dentro do prazo estabelecido no item 15.4.1.3, ensejará a aplicação de penalidades descritas no item 21 deste edital.

13.5. A contratação formalizar-se-á mediante instrumento particular, observadas as cláusulas e condições deste Edital, da Ata de Registro de Preços e da proposta vencedora.

13.6. A licitante que tenha seu preço registrado estará obrigada a cumprir todas as condições dispostas na Ata de Registro de Preços (ANEXO II).

14 - DO CONTRATO, DA GESTÃO E DA FISCALIZAÇÃO

14.1. O adjudicatário será convocado para assinar o instrumento contratual, devendo assinar e restituí-lo ao Tribunal de Justiça do estado do Tocantins no prazo de 05 (cinco) dias corridos, podendo este prazo ser prorrogado, a critério da Administração, por igual período e por uma vez, desde que ocorra motivo justificado.

14.2. No ato de assinatura do contrato, a Contratada deverá atender as disposições da Portaria nº 97/2010, quanto à verificação da regularidade fiscal. Se qualquer das certidões apresentadas na fase de habilitação do procedimento licitatório expirar sua validade antes da data de assinatura dos contratos ou de seus aditivos, deverá a mesma ser atualizada.

14.2.1. Integra o presente Edital a **minuta do Contrato (ANEXO III)** que **deverá ser assinada eletronicamente** pela licitante vencedora, no prazo de até 05 (cinco) dias corridos contados da sua disponibilização no Sistema Eletrônico de Informação.

14.2.2. Para efetivar a assinatura eletrônica do Contrato, a licitante vencedora deverá estar cadastrada no Sistema Eletrônico de Informação deste Tribunal.

14.2.3. Caso não possua o referido cadastro, será enviado link de página da internet, para o e-mail do responsável pela assinatura do Contrato, como forma de se implementar a assinatura eletrônica.

14.3. O contrato a ser firmado vigorará nos termos do disposto no item 9 do Termo de Referência (ANEXO I).

14.4. As disposições acerca da gestão e fiscalização contratual estão dispostas no item 4 do Termo de referência (ANEXO I) do edital.

14.5. No ato de emissão da nota de empenho, a licitante deverá atender as disposições da Portaria nº 97, de 2010, do Tribunal de Justiça do Estado do Tocantins, quanto à verificação da regularidade fiscal. Se qualquer das certidões apresentadas na fase de habilitação do procedimento licitatório expirar sua validade antes da data de emissão da nota de empenho, deverá ser atualizada;

14.6. É facultado à Administração, quando à adjudicatária convocada não retirar a nota de empenho, no prazo de 02 (dois) dias úteis, convocar outra licitante, obedecida à ordem de classificação, para retirá-la, após, comprovados os requisitos de habilitação, feita a negociação e aceita a proposta ou revogar o certame.

14.7. A nota de empenho vigorará a partir da emissão, ficando adstrita ao crédito orçamentário conforme disposto no art. 57 da Lei nº 8.666, de 1993, ressalvado o prazo de garantia dos produtos.

14.8. O acompanhamento (gestão) e fiscalização serão realizados por servidor designado pela administração.

14.9. A atuação ou a eventual omissão da fiscalização durante a realização dos trabalhos, não poderá ser invocada para eximir a licitante da responsabilidade no fornecimento dos produtos.

14.10. A fiscalização será sob o aspecto qualitativo e quantitativo, devendo ser anotado, em registro próprio as falhas detectadas, e comunicadas ao gestor do contrato todas as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte da licitante.

14.11. A comunicação entre o fiscal do contrato e a licitante será realizada através de correspondência oficial e anotações ou registros no mesmo processo que trata da contratação dos objetos.

14.12. Quando houver necessidade de emitir notificações para a licitante, o gestor deverá dar conhecimento ao Diretor Administrativo para que este pratique o ato.

14.13. Demais atribuições e responsabilidades do gestor de contratos no âmbito do TJ/TO estão disciplinadas pelo Decreto Judiciário nº 291, de 2009 e Portaria nº 255, de 2009 TJ/TO.

15 - DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

15.1. Os critérios de recebimento e aceitação do objeto encontram-se especificados nos itens 6 do Termo de Referência (anexo I do Edital).

16 - DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

16.1. As obrigações das partes são aquelas especificadas no item 11.12 do Termo de Referência (anexo I do Edital).

17 - DO PAGAMENTO

17.1. As condições acerca do pagamento são as estabelecidas no item 7 do Termo de Referência(anexo I do Edital).

18 - DA ATUALIZAÇÃO MONETÁRIA

18.1. Ocorrendo atraso no pagamento, e desde que para tal não tenha concorrido de alguma forma a adjudicatária, haverá incidência de atualização monetária sobre o valor devido, pela variação acumulada do Índice Geral de Preços - Disponibilidade Interna (IGP-DI), coluna dois, publicado pela Fundação Getúlio Vargas, ocorrida entre a data final prevista para o pagamento e a data de sua efetiva realização.

19 - DAS SANÇÕES ADMINISTRATIVAS

19.1. A empresa que, convocada dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar a documentação exigida para o certame ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedida de licitar e contratar com a Administração Pública do Estado do Tocantins e será descredenciada no Sistema de Cadastramento

Unificado de Fornecedores (Sicaf), pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais.

19.2. Subsidiariamente, nos termos do art. 87 da Lei nº 8.666/93, pela inexecução total ou parcial das condições estabelecidas neste instrumento, o Poder Judiciário do Estado do Tocantins poderá, garantida a prévia defesa da empresa, que deverá ser apresentada no prazo de 5 (cinco) dias úteis a contar da sua notificação, aplicar, sem prejuízo das responsabilidades penal e civil, as seguintes sanções:

I - Advertência, por escrito, quando a empresa deixar de atender quaisquer indicações aqui constantes;

II - Multa compensatória/indenizatória no percentual de 5% (cinco por cento) calculado sobre o valor contratado;

III - Suspensão temporária de participação em licitação e impedimento de contratar com o Poder Judiciário do Estado do Tocantins, pelo prazo de até 2 (dois) anos; e

IV - Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

19.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pela empresa, a esta será aplicada multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor do contrato ou instrumento equivalente, por dia de atraso, limitada a 10% (dez por cento) do valor inadimplido.

19.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhido ao Fundo Especial de Modernização e Aprimoramento do Poder Judiciário FUNJURIS, dentro do prazo de 5 (cinco) dias úteis após a respectiva notificação.

19.5. Caso não seja paga no prazo previsto no subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado pelo Poder Judiciário do Estado do Tocantins ou cobrada judicialmente.

19.6. Além das penalidades citadas, a empresa ficará sujeita, ainda, no que couber, às demais penalidades referidas no Capítulo IV da Lei nº 8.666/93."

19.7. As demais sanções previstas no item 10 do Termo de Referência (Anexo I do Edital).

20 - DO PEDIDO DE ESCLARECIMENTO E DA IMPUGNAÇÃO AO EDITAL

20.1. Qualquer interessado, antes de decidir participar deste Pregão Eletrônico, deverá providenciar exaustivo estudo do inteiro teor do Edital e apresentar, à CPL, as dúvidas e impugnações (inclusive as correlatas a eventuais irrazoabilidades, desproporcionalidades e/ou omissões) que entender existentes neste instrumento.

20.2. Ao participar desta licitação, a licitante estará se declarando ciente de que as condições editalícias, descrições de produtos, condições de fornecimento e outras fórmulas destinam-se a garantir, nos termos Lei, transparência, objetividade, certeza jurídica e isonomia de tratamento a todos os participantes bem como à obtenção de eficácia e celeridade para o processo seletivo do menor preço (ou maior desconto) e da melhor proposta.

20.3. Os pedidos de esclarecimentos deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico no e-mail:cpl@tjto.jus.br

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

20.3.2. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema eletrônico e vincularão os participantes e a administração.

20.4. Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este instrumento convocatório, mediante petição a ser encaminhada por meio eletrônico no e-mail:cpl@cnj.jus.br ou por petição dirigida ou protocolada na Secretaria de Processos Administrativos (SPA) do Tribunal de Justiça do Estado do Tocantins, localizada no Palácio da Justiça Rio Tocantins, Praça dos Girassóis, s/nº Centro - Palmas - Tocantins / CEP: 77015-007, horário de atendimento ao público: das 12:00 às 18:00 horas.

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

20.4.2. Acolhida a impugnação, será designada nova data para a realização do certame.

21 - DAS DISPOSIÇÕES GERAIS

21.1. O Edital estará à disposição dos interessados na Comissão Permanente de Licitação, localizada no Anexo I do Tribunal de Justiça do Estado do Tocantins (Edifício Amaro Empresarial), situado na Quadra 103 Norte, Rua NO-11, Lote 2, 7º Andar, Plano Diretor Norte, Palmas/TO, CEP 77.001-036, Telefone (63) 3218-4590, nos dias úteis, das 12h às 18h, e na internet para download, nos endereços eletrônicos: www.comprasgovernamentais.gov.br e http://www.tjto.jus.br/index.php/cidadao/licitacoes

21.2. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

21.3. Não se admitirá um mesmo profissional como representante de mais de uma licitante;

21.4. O pregoeiro poderá, no julgamento da habilitação e das propostas, 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 aos licitantes, e lhes atribuirá validade e eficácia para fins de habilitação e classificação, observado o disposto na Lei nº 9.784, de 29 de janeiro de 1999.

21.5. É facultado ao Pregoeiro ou à autoridade superior, em qualquer fase desta licitação, promover diligências destinadas a esclarecer ou complementar a instrução de assunto relacionado ao presente Edital.

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

21.7. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

21.8. 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.

21.9. 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.

21.10. 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.

21.11. O pregoeiro ou autoridade superior poderão subsidiar-se em pareceres emitidos por técnicos ou especialistas no assunto objeto desta licitação.

23.12. Em nenhuma hipótese a licitante/adjudicatária poderá alegar desconhecimento, incompreensão, dúvida ou esquecimento de qualquer detalhe relativo à execução do objeto, arcando com quaisquer ônus decorrentes desses fatos.

21.13. A critério do Tribunal de Justiça do Estado do Tocantins a presente licitação poderá ser:

21.13.1. Adiada, por conveniência exclusiva da Administração;

21.13.2. Revogada, a juízo da Administração, se considerada inoportuna ou inconveniente ao interesse público, decorrente de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta;

21.13.3. Anulada, se houver ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado.

21.13.3.1. A anulação do procedimento licitatório induz à da contratação

21.14. A licitante é responsável administrativa, civil e penalmente pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase desta licitação.

21.15. O Tribunal de Justiça do Estado do Tocantins reserva-se o direito de considerar válidas comunicações enviadas aos licitantes, aos adjudicatários e a quaisquer outros interessados pelos endereços, inclusive eletrônicos, registrados nos autos e/ou no Sistema SICAF (mantido pelo Poder Executivo Federal).

21.16. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

ANEXO I - Termo de Referência

ANEXO "A" do Termo de Referência - Minuta do Termo de Recebimento Provisório de Bens não Permanentes

ANEXO "B" do Termo de Referência - Minuta do Termo de Recebimento Definitivo de Bens não Permanentes

ANEXO "C" do Termo de Referência - Acordo de Nível de Serviço

ANEXO II – Minuta da Ata de Registro de Preços

ANEXO III – Minuta do Contrato

ANEXO IV - Minuta – Portaria de Designação de Gestor do Contrato

21.17. Os casos omissos serão resolvidos pelo (a) Pregoeiro(a), que decidirá com base na legislação em vigor.

21.18. Para dirimir as questões relativas ao presente Edital, elege-se como foro competente o de Palmas – TO, com exclusão de qualquer outro.

Palmas, 01 de julho de 2021

Agno Paixão Saraiva

Pregoeiro

ANEXO I

Termo de Referência Nº 192 / 2021 - PRESIDÊNCIA/DIGER/DTINF/GABDTI

1. OBJETO

1.1. Visa o presente Termo de Referência registrar preços, objetivando a renovação e a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – Versão Business Select, incluindo atualizações e suporte técnico pelo período de 36 (trinta e seis) meses, para atender as demandas do Poder Judiciário do Estado do Tocantins, conforme as especificações e quantidades estabelecidas neste documento, mediante licitação regida pelo Decreto Judiciário nº 6 de 14 de janeiro de 2020.

Item	Descrição	CATMAT / CATSER	Unidade	Qtde.	Valor Estimado Unitário	Total
1	Renovação de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select.	350949	Un.	2.850	R$ 113,19	R$ 322.591,50
2	Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select.	350949	Un.	650	R$ 117,20	R$ 76.180,00
Total Geral						R$ 398.771,50

2. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

2.1. Renovação de licenças de solução corporativa de antivírus

2.1.1. Características Gerais

2.1.1.1. Todas as licenças fornecidas terão validade de 36 (trinta e seis) meses para atualizações inerentes ao produto.

2.1.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

2.1.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

2.1.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para o Contratante além daquele já cotado na proposta.

2.1.2. Servidor de Administração e Console Administrativa

2.1.2.1. Compatibilidade:

2.1.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

2.1.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

2.1.2.1.3. Microsoft Windows Server 2016 x64.

2.1.2.1.4. Microsoft Windows Server 2019 x64.

2.1.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

2.1.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

2.1.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

2.1.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

2.1.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

2.1.2.2. Características:

2.1.2.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC.

2.1.2.2.2. Console deve ser baseada no modelo cliente/servidor.

2.1.2.2.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.

2.1.2.2.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.

2.1.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

2.1.2.2.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM.

2.1.2.2.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores.

2.1.2.2.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory.

2.1.2.2.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.

2.1.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

2.1.2.2.11. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada.

2.1.2.2.12. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas.

2.1.2.2.13. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas.

2.1.2.2.14. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador.

2.1.2.2.15. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle.

2.1.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

2.1.2.2.17. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus.

2.1.2.2.18. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança.

2.1.2.2.19. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede.

2.1.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

2.1.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

2.1.2.2.22. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes.

2.1.2.2.23. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

2.1.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

2.1.2.2.25. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

2.1.2.2.25.1. Nome do computador.

2.1.2.2.25.2. Nome do domínio.

2.1.2.2.25.3. Range de IP.

2.1.2.2.25.4. Sistema Operacional.

2.1.2.2.25.5. Máquina virtual.

2.1.2.2.26. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas.

2.1.2.2.27. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional.

2.1.2.2.28. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção.

2.1.2.2.29. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção.

2.1.2.2.30. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente.

2.1.3.1.2. Microsoft Windows 8 Professional/Enterprise.

2.1.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

2.1.3.1.4. Microsoft Windows 10 Professional/Enterprise.

2.1.3.2. Características:

2.1.3.2.1. Deve prover as seguintes proteções:

2.1.3.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.1.3.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus).

2.1.3.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos).

2.1.3.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza.

2.1.3.2.1.5. Firewall com IDS.

2.1.3.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus).

2.1.3.2.1.7. Controle de dispositivos externos.

2.1.3.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

2.1.3.2.1.9. Controle de acesso a sites por horário.

2.1.3.2.1.10. Controle de acesso a sites por usuários.

2.1.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

2.1.3.2.1.12. Controle de execução de aplicativos.

2.1.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

2.1.3.2.2.Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.1.3.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

2.1.3.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

2.1.3.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (exemplo: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.1.3.2.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas.

2.1.3.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

2.1.3.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.1.3.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.1.3.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas.

2.1.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

2.1.3.2.12. Capacidade de verificar objetos usando heurística.

2.1.3.2.13. Capacidade de agendar uma pausa na verificação.

2.1.3.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias.

2.1.3.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

2.1.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.1.3.2.16.1. Perguntar o que fazer, ou;

2.1.3.2.16.2. Bloquear acesso ao objeto.

2.1.3.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.3.2.16.2.2. Caso positivo de desinfecção:

2.1.3.2.16.2.2.1. Restaurar o objeto para uso.

2.1.3.2.16.2.3. Caso negativo de desinfecção:

2.1.3.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.1.3.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI.

2.1.3.2.19. Capacidade de verificar links inseridos em e-mails contra phishings.

2.1.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

2.1.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

2.1.3.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

2.1.3.2.22.1. Perguntar o que fazer, ou;

2.1.3.2.22.2. Bloquear o e-mail.

2.1.3.2.22.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.3.2.22.2.2. Caso positivo de desinfecção:

2.1.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

2.1.3.2.22.2.3. Caso negativo de desinfecção:

2.1.3.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.3.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

2.1.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

2.1.3.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.

2.1.3.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script etc.), usando heurísticas.

2.1.3.2.27. Deve ter suporte total ao protocolo Ipv6.

2.1.3.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail.

2.1.3.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

2.1.3.2.29.1. Perguntar o que fazer, ou;

2.1.3.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.1.3.2.29.3. Permitir acesso ao objeto.

2.1.3.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

2.1.3.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

2.1.3.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

2.1.3.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

2.1.3.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.

2.1.3.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

2.1.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

2.1.3.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

2.1.3.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica.

2.1.3.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

2.1.3.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.1.3.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas.

2.1.3.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.1.3.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

2.1.3.2.39.1. Discos de armazenamento locais.

2.1.3.2.39.2. Armazenamento removível.

2.1.3.2.39.3. Impressoras.

2.1.3.2.39.4. CD/DVD.

2.1.3.2.39.5. Drives de disquete.

2.1.3.2.39.6. Modems.

2.1.3.2.39.7. Dispositivos de fita.

2.1.3.2.39.8. Dispositivos multifuncionais.

2.1.3.2.39.9. Leitores de smart card.

2.1.3.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile etc.).

2.1.3.2.39.11. Wi-Fi.

2.1.3.2.39.12. Adaptadores de rede externos.

2.1.3.2.39.13. Dispositivos MP3 ou smartphones.

2.1.3.2.39.14. Dispositivos Bluetooth.

2.1.3.2.39.15. Câmeras e Scanners.

2.1.3.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário.

2.1.3.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

2.1.3.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

2.1.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

2.1.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

2.1.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

2.1.3.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

2.1.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.1.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.1.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

2.1.3.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.

2.1.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.1.3.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.1.3.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

2.1.3.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

2.1.3.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.1.3.2.54. Capacidade de integração com o Windows Defender Security Center.

2.1.3.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).

2.1.3.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

2.1.4. Estações Mac OS X

2.1.4.1. Compatibilidade:

2.1.4.1.1. OS X 10.9 (Mavericks).

2.1.4.1.2. OS X 10.10 (Yosemite).

2.1.4.1.3. OS X 10.11 (El Capitan).

2.1.4.1.4. macOS 10.12 (Sierra).

2.1.4.1.5. macOS 10.13 (High Sierra).

2.1.4.1.6. macOS 10.14 (Mojave).

2.1.4.1.7. macOS 10.15 (Catalina).

2.1.4.1.8. macOS 11.0 (Big Sur).

2.1.4.2. Características:

2.1.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.1.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https.

2.1.4.2.3. Possuir módulo de bloqueio a ataques na rede.

2.1.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador.

2.1.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

2.1.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

2.1.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

2.1.4.2.8. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.1.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

2.1.4.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

2.1.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

2.1.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

2.1.4.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.1.4.2.14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

2.1.4.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.1.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

2.1.4.2.17. Capacidade de verificar objetos usando heurística.

2.1.4.2.18. Capacidade de agendar uma pausa na verificação.

2.1.4.2.19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.1.4.2.19.1. Perguntar o que fazer, ou;

2.1.4.2.19.2. Bloquear acesso ao objeto.

2.1.4.2.19.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.4.2.19.3.1. Caso positivo de desinfecção:

2.1.4.2.19.3.1.1. Restaurar o objeto para uso.

2.1.4.2.19.3.2. Caso negativo de desinfecção:

2.1.4.2.19.3.2.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.4.2.20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.1.4.2.21. Capacidade de verificar arquivos de formato de email.

2.1.4.2.22. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, parar o antivírus e iniciar o antivírus pela linha de comando.

2.1.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

2.1.5. Estações Linux

2.1.5.1. Compatibilidade:

2.1.5.1.1. Plataforma 32 bits:

2.1.5.1.1.1. Ubuntu 16.04 LTS

2.1.5.1.1.2. Red Hat® Enterprise Linux® 6.7

2.1.5.1.1.3. CentOS-6.7

2.1.5.1.1.4. Debian GNU / Linux 9.4

2.1.5.1.2. Plataforma 64 bits:

2.1.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

2.1.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

2.1.5.1.2.3. CentOS-6.7, 7.2, 8.0

2.1.5.1.2.4. Debian GNU / Linux 9.4, 10.1

2.1.5.1.2.5. OracleLinux 7.3, 8

2.1.5.1.2.6. SUSE® Linux Enterprise Server 15

2.1.5.1.2.7. openSUSE® 15

2.1.5.1.2.8. Amazon Linux AMI

2.1.5.2. Características

2.1.5.2.1. Deve prover as seguintes proteções:

2.1.5.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.1.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

2.1.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

2.1.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

2.1.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

2.1.5.2.7. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.1.5.2.8. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.1.5.2.9. Capacidade de criar exclusões por local, máscara e nome da ameaça.

2.1.5.2.10. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.1.5.2.11. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

2.1.5.2.12. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers.

2.1.5.2.13. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

2.1.5.2.13.1. Alta.

2.1.5.2.13.2. Média.

2.1.5.2.13.3. Baixa.

2.1.5.2.13.4. Recomendado.

2.1.5.2.14. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

2.1.5.2.15. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos. desinfecção ou remoção de objetos infectados.

2.1.5.2.16. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

2.1.5.2.17. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.1.5.2.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.1.5.2.19. Capacidade de verificar objetos usando heurística.

2.1.5.2.20. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.1.5.2.21. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

2.1.6. Servidores Windows

2.1.6.1. Compatibilidade:

2.1.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

2.1.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

2.1.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

2.1.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

2.1.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

2.1.6.1.6. Microsoft Windows Server 2016.

2.1.6.1.7. Microsoft Windows Server 2019.

2.1.6.2. Características:

2.1.6.2.1. Deve prover as seguintes proteções:

2.1.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.1.6.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus.

2.1.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

2.1.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

2.1.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.1.6.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.1.6.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.1.6.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.1.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

2.1.6.2.4.3. Leitura de configurações.

2.1.6.2.4.4. Modificação de configurações.

2.1.6.2.4.5. Gerenciamento de Backup e Quarentena.

2.1.6.2.4.6. Visualização de relatórios.

2.1.6.2.4.7. Gerenciamento de relatórios.

2.1.6.2.4.8. Gerenciamento de chaves de licença.

2.1.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

2.1.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

2.1.6.2.6. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede.

2.1.6.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros etc.).

2.1.6.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS).

2.1.6.2.9. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares.

2.1.6.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

2.1.6.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.

2.1.6.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

2.1.6.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

2.1.6.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.1.6.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.1.6.2.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.1.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

2.1.6.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (exemplo: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários etc.).

2.1.6.2.19. Capacidade de verificar objetos usando heurística.

2.1.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

2.1.6.2.21. Capacidade de agendar uma pausa na verificação.

2.1.6.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

2.1.6.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.1.6.2.23.1. Perguntar o que fazer, ou;

2.1.6.2.23.2. Bloquear acesso ao objeto.

2.1.6.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.6.2.23.2.2. Caso positivo de desinfecção:

2.1.6.2.23.2.2.1. Restaurar o objeto para uso.

2.1.6.2.23.3. Caso negativo de desinfecção:

2.1.6.2.23.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.6.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.1.6.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.1.6.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

2.1.6.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

2.1.6.2.28. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

2.1.6.2.29. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.1.6.2.30. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

2.1.7. Servidores Linux

2.1.7.1. Compatibilidade:

2.1.7.1.1. Plataforma 32 bits:

2.1.7.1.1.1. Ubuntu 16.04 LTS.

2.1.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

2.1.7.1.1.3. CentOS-6.7.

2.1.7.1.1.4. Debian GNU / Linux 9.4.

2.1.7.1.2. Plataforma 64 bits:

2.1.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

2.1.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

2.1.7.1.2.3. CentOS-6.7, 7.2, 8.0.

2.1.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

2.1.7.1.2.5. OracleLinux 7.3, 8.

2.1.7.1.2.6. SUSE® Linux Enterprise Server 15.

2.1.7.1.2.7. openSUSE® 15.

2.1.7.1.2.8. Amazon Linux AMI.

2.1.7.2. Características:

2.1.7.2.1. Deve prover as seguintes proteções:

2.1.7.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.1.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

2.1.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

2.1.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

2.1.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

2.1.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

2.1.7.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.1.7.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.1.7.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.1.7.2.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

2.1.7.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

2.1.7.2.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

2.1.7.2.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

2.1.7.2.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.1.7.2.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.1.7.2.7. Capacidade de verificar objetos usando heurística.

2.1.7.2.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.1.7.2.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

2.1.7.2.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

2.1.8. Smartphones e tablets

2.1.8.1. Compatibilidade:

2.1.8.1.1. Dispositivos com os sistemas operacionais:

2.1.8.1.1.1. Android 4.2 – 11.

2.1.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

2.1.8.2. Características:

2.1.8.2.1. Deve prover as seguintes proteções:

2.1.8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

2.1.8.2.1.2. Proteção contra adware e autodialers.

2.1.8.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.

2.1.8.2.1.4. Arquivos abertos no smartphone.

2.1.8.2.1.5. Programas instalados usando a interface do smartphone

2.1.8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento.

2.1.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

2.1.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

2.1.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

2.1.8.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.

2.1.8.2.6. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha.

2.1.8.2.7. Deverá ter firewall pessoal (Android).

2.1.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

2.1.8.2.9. Capacidade de enviar comandos remotamente de:

2.1.8.2.9.1. Localizar.

2.1.8.2.9.2. Bloquear.

2.1.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

2.1.8.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos.

2.1.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

2.1.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

2.1.8.2.14. Capacidade de localizar o dispositivo quando necessário.

2.1.8.2.15. Permitir atualização das definições quando estiver em "roaming".

2.1.8.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus.

2.1.8.2.17. Deve permitir verificar somente arquivos executáveis.

2.1.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

2.1.8.2.19. Capacidade de agendar uma verificação.

2.1.8.2.20. Capacidade de enviar URL de instalação por e-mail.

2.1.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

2.1.8.2.22. Capacidade de executar as seguintes ações caso a desinfecção falhe:

2.1.8.2.22.1. Deletar.

2.1.8.2.22.2. Ignorar.

2.1.8.2.22.3. Quarentenar.

2.1.8.2.22.4. Perguntar ao usuário.

2.1.9. Gerenciamento de dispositivos móveis (MDM):

2.1.9.1. Compatibilidade:

2.1.9.1.1. Android 4.2 – 11.

2.1.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

2.1.9.2. Características:

2.1.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

2.1.9.2.2. Capacidade de ajustar as configurações de:

2.1.9.2.2.1. Sincronização de e-mail.

2.1.9.2.2..2. Uso de aplicativos.

2.1.9.2.2.3. Senha do usuário.

2.1.9.2.2.4. Criptografia de dados.

2.1.9.2.2.5. Conexão de mídia removível.

2.1.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

2.1.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

2.1.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

2.1.9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS.

2.1.9.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento.

2.1.9.2.8. Permitir sincronização com perfil do "Touch Down".

2.1.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

2.1.9.2.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual.

2.1.9.2.11. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

2.2. Aquisição de licenças de solução corporativa de antivírus

2.2.1. Características Gerais

2.2.1.1. Todas as licenças fornecidas terão validade de 36 (trinta e seis) meses para atualizações inerentes ao produto.

2.2.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

2.2.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

2.2.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para o Contratante além daquele já cotado na proposta.

2.2.2. Servidor de Administração e Console Administrativa

2.2.2.1. Compatibilidade:

2.2.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

2.2.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

2.2.2.1.3. Microsoft Windows Server 2016 x64.

2.2.2.1.4. Microsoft Windows Server 2019 x64.

2.2.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

2.2.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

2.2.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

2.2.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

2.2.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

2.2.2.2. Características:

2.2.2.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC.

2.2.2.2.2. Console deve ser baseada no modelo cliente/servidor.

2.2.2.2.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.

2.2.2.2.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.

2.2.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

2.2.2.2.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM.

2.2.2.2.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores.

2.2.2.2.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory.

2.2.2.2.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.

2.2.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

2.2.2.2.11. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada.

2.2.2.2.12. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas.

2.2.2.2.13. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas.

2.2.2.2.14. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador.

2.2.2.2.15. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle.

2.2.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

2.2.2.2.17. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus.

2.2.2.2.18. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança.

2.2.2.2.19. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede.

2.2.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

2.2.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

2.2.2.2.22. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes.

2.2.2.2.23. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

2.2.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

2.2.2.2.25. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

2.2.2.2.25.1. Nome do computador.

2.2.2.2.25.2. Nome do domínio.

2.2.2.2.25.3. Range de IP.

2.2.2.2.25.4. Sistema Operacional.

2.2.2.2.25.5. Máquina virtual.

2.2.2.2.26. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas.

2.2.2.2.27. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional.

2.2.2.2.28. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção.

2.2.2.2.29. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção.

2.2.2.2.30. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente.

2.2.2.2.31. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias etc.

2.2.2.2.32. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos.

2.2.2.2.33. Deve fornecer as seguintes informações dos computadores:

2.2.2.2.33.1. Se o antivírus está instalado.

2.2.2.2.33.2. Se o antivírus está iniciado.

2.2.2.2.33.3. Se o antivírus está atualizado.

2.2.2.2.33.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo.

2.2.2.2.33.5. Minutos/horas desde a última atualização de vacinas.

2.2.2.2.33.6. Data e horário da última verificação executada na máquina.

2.2.2.2.33.7. Versão do antivírus instalado na máquina.

2.2.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças.

2.2.2.2.33.9. Data e horário de quando a máquina foi ligada.

2.2.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina.

2.2.2.2.33.11. Nome do computador.

2.2.2.2.33.12. Domínio ou grupo de trabalho do computador.

2.2.2.2.33.13. Data e horário da última atualização de vacinas.

2.2.2.2.33.14. Sistema operacional com Service Pack.

2.2.2.2.33.15. Quantidade de processadores.

2.2.2.2.33.16. Quantidade de memória RAM.

2.2.2.2.33.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory).

2.2.2.2.33.18. Endereço IP.

2.2.2.2.33.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.

2.2.2.2.33.20. Atualizações do Windows Updates instaladas.

2.2.2.2.33.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD.

2.2.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina.

2.2.2.2.34. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las.

2.2.2.2.35. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

2.2.2.2.35.1. Alteração de Gateway Padrão.

2.2.2.2.35.2. Alteração de subrede.

2.2.2.2.35.3. Alteração de domínio.

2.2.2.2.35.4. Alteração de servidor DHCP.

2.2.2.2.35.5. Alteração de servidor DNS.

2.2.2.2.35.6. Alteração de servidor WINS.

2.2.2.2.35.7. Alteração de subrede.

2.2.2.2.35.8. Resolução de Nome.

2.2.2.2.35.9. Disponibilidade de endereço de conexão SSL.

2.2.2.2.36. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet.

2.2.2.2.37. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes.

2.2.2.2.38. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus.

2.2.2.2.39. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos.

2.2.2.2.40. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede.

2.2.2.2.41. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.

2.2.2.2.42. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

2.2.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos.

2.2.2.2.44. Capacidade de enviar e-mails para contas específicas em caso de algum evento.

2.2.2.2.45. Listar em um único local, todos os computadores não gerenciados na rede.

2.2.2.2.46. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes.

2.2.2.2.47. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

2.2.2.2.48. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação etc.), inclusive de máquinas que estejam em subnets diferentes do servidor.

2.2.2.2.49. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo).

2.2.2.2.50. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador.

2.2.2.2.51. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (exemplo: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint).

2.2.2.2.52. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação.

2.2.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

2.2.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

2.2.2.2.55. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

2.2.2.2.55.1. Nome do vírus.

2.2.2.2.55.2. Nome do arquivo infectado.

2.2.2.2.55.3. Data e hora da detecção.

2.2.2.2.55.4. Nome da máquina ou endereço IP.

2.2.2.2.55.5. Ação realizada.

2.2.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

2.2.2.2.57. Capacidade de listar updates nas máquinas com o respectivo link para download.

2.2.2.2.58. Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração.

2.2.2.2.59. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante.

2.2.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente.

2.2.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2.2.3. Estações Windows

2.2.3.1. Compatibilidade:

2.2.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate.

2.2.3.1.2. Microsoft Windows 8 Professional/Enterprise.

2.2.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

2.2.3.1.4. Microsoft Windows 10 Professional/Enterprise.

2.2.3.2. Características:

2.2.3.2.1. Deve prover as seguintes proteções:

2.2.3.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.3.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus).

2.2.3.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos).

2.2.3.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza.

2.2.3.2.1.5. Firewall com IDS.

2.2.3.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus).

2.2.3.2.1.7. Controle de dispositivos externos.

2.2.3.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

2.2.3.2.1.9. Controle de acesso a sites por horário.

2.2.3.2.1.10. Controle de acesso a sites por usuários.

2.2.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

2.2.3.2.1.12. Controle de execução de aplicativos.

2.2.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

2.2.3.2.2.Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.2.3.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

2.2.3.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

2.2.3.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (exemplo: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.2.3.2.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas.

2.2.3.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

2.2.3.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.2.3.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.2.3.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas.

2.2.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

2.2.3.2.12. Capacidade de verificar objetos usando heurística.

2.2.3.2.13. Capacidade de agendar uma pausa na verificação.

2.2.3.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias.

2.2.3.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

2.2.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.2.3.2.16.1. Perguntar o que fazer, ou;

2.2.3.2.16.2. Bloquear acesso ao objeto.

2.2.3.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.3.2.16.2.2. Caso positivo de desinfecção:

2.2.3.2.16.2.2.1. Restaurar o objeto para uso.

2.2.3.2.16.2.3. Caso negativo de desinfecção:

2.2.3.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.2.3.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI.

2.2.3.2.19. Capacidade de verificar links inseridos em e-mails contra phishings.

2.2.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

2.2.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

2.2.3.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

2.2.3.2.22.1. Perguntar o que fazer, ou;

2.2.3.2.22.2. Bloquear o e-mail.

2.2.3.2.22.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.3.2.22.2.2. Caso positivo de desinfecção:

2.2.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

2.2.3.2.22.2.3. Caso negativo de desinfecção:

2.2.3.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.3.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

2.2.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

2.2.3.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.

2.2.3.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script etc.), usando heurísticas.

2.2.3.2.27. Deve ter suporte total ao protocolo Ipv6.

2.2.3.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail.

2.2.3.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

2.2.3.2.29.1. Perguntar o que fazer, ou;

2.2.3.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.2.3.2.29.3. Permitir acesso ao objeto.

2.2.3.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

2.2.3.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

2.2.3.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

2.2.3.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

2.2.3.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.

2.2.3.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

2.2.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

2.2.3.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

2.2.3.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica.

2.2.3.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

2.2.3.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.2.3.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas.

2.2.3.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.2.3.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

2.2.3.2.39.1. Discos de armazenamento locais.

2.2.3.2.39.2. Armazenamento removível.

2.2.3.2.39.3. Impressoras.

2.2.3.2.39.4. CD/DVD.

2.2.3.2.39.5. Drives de disquete.

2.2.3.2.39.6. Modems.

2.2.3.2.39.7. Dispositivos de fita.

2.2.3.2.39.8. Dispositivos multifuncionais.

2.2.3.2.39.9. Leitores de smart card.

2.2.3.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile etc.).

2.2.3.2.39.11. Wi-Fi.

2.2.3.2.39.12. Adaptadores de rede externos.

2.2.3.2.39.13. Dispositivos MP3 ou smartphones.

2.2.3.2.39.14. Dispositivos Bluetooth.

2.2.3.2.39.15. Câmeras e Scanners.

2.2.3.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário.

2.2.3.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

2.2.3.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

2.2.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

2.2.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

2.2.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

2.2.3.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

2.2.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.2.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.2.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

2.2.3.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.

2.2.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.2.3.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.2.3.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

2.2.3.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

2.2.3.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.2.3.2.54. Capacidade de integração com o Windows Defender Security Center.

2.2.3.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).

2.2.3.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

2.2.4. Estações Mac OS X

2.2.4.1. Compatibilidade:

2.2.4.1.1. OS X 10.9 (Mavericks).

2.2.4.1.2. OS X 10.10 (Yosemite).

2.2.4.1.3. OS X 10.11 (El Capitan).

2.2.4.1.4. macOS 10.12 (Sierra).

2.2.4.1.5. macOS 10.13 (High Sierra).

2.2.4.1.6. macOS 10.14 (Mojave).

2.2.4.1.7. macOS 10.15 (Catalina).

2.2.4.1.8. macOS 11.0 (Big Sur).

2.2.4.2. Características:

2.2.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https.

2.2.4.2.3. Possuir módulo de bloqueio a ataques na rede.

2.2.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador.

2.2.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

2.2.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

2.2.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

2.2.4.2.8. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.2.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

2.2.4.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

2.2.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

2.2.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

2.2.4.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.2.4.2.14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

2.2.4.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.2.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

2.2.4.2.17. Capacidade de verificar objetos usando heurística.

2.2.4.2.18. Capacidade de agendar uma pausa na verificação.

2.2.4.2.19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.2.4.2.19.1. Perguntar o que fazer, ou;

2.2.4.2.19.2. Bloquear acesso ao objeto.

2.2.4.2.19.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.4.2.19.3.1. Caso positivo de desinfecção:

2.2.4.2.19.3.1.1. Restaurar o objeto para uso.

2.2.4.2.19.3.2. Caso negativo de desinfecção:

2.2.4.2.19.3.2.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.4.2.20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.2.4.2.21. Capacidade de verificar arquivos de formato de email.

2.2.4.2.22. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, parar o antivírus e iniciar o antivírus pela linha de comando.

2.2.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

2.2.5. Estações Linux

2.2.5.1. Compatibilidade:

2.2.5.1.1. Plataforma 32 bits:

2.2.5.1.1.1. Ubuntu 16.04 LTS

2.2.5.1.1.2. Red Hat® Enterprise Linux® 6.7

2.2.5.1.1.3. CentOS-6.7

2.2.5.1.1.4. Debian GNU / Linux 9.4

2.2.5.1.2. Plataforma 64 bits:

2.2.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

2.2.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

2.2.5.1.2.3. CentOS-6.7, 7.2, 8.0

2.2.5.1.2.4. Debian GNU / Linux 9.4, 10.1

2.2.5.1.2.5. OracleLinux 7.3, 8

2.2.5.1.2.6. SUSE® Linux Enterprise Server 15

2.2.5.1.2.7. openSUSE® 15

2.2.5.1.2.8. Amazon Linux AMI

2.2.5.2. Características

2.2.5.2.1. Deve prover as seguintes proteções:

2.2.5.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

2.2.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

2.2.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

2.2.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

2.2.5.2.7. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.2.5.2.8. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.2.5.2.9. Capacidade de criar exclusões por local, máscara e nome da ameaça.

2.2.5.2.10. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.2.5.2.11. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

2.2.5.2.12. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers.

2.2.5.2.13. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

2.2.5.2.13.1. Alta.

2.2.5.2.13.2. Média.

2.2.5.2.13.3. Baixa.

2.2.5.2.13.4. Recomendado.

2.2.5.2.14. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

2.2.5.2.15. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos. desinfecção ou remoção de objetos infectados.

2.2.5.2.16. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

2.2.5.2.17. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.2.5.2.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.2.5.2.19. Capacidade de verificar objetos usando heurística.

2.2.5.2.20. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.2.5.2.21. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

2.2.6. Servidores Windows

2.2.6.1. Compatibilidade:

2.2.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

2.2.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

2.2.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

2.2.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

2.2.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

2.2.6.1.6. Microsoft Windows Server 2016.

2.2.6.1.7. Microsoft Windows Server 2019.

2.2.6.2. Características:

2.2.6.2.1. Deve prover as seguintes proteções:

2.2.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.6.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus.

2.2.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

2.2.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

2.2.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.2.6.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.2.6.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.2.6.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.2.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

2.2.6.2.4.3. Leitura de configurações.

2.2.6.2.4.4. Modificação de configurações.

2.2.6.2.4.5. Gerenciamento de Backup e Quarentena.

2.2.6.2.4.6. Visualização de relatórios.

2.2.6.2.4.7. Gerenciamento de relatórios.

2.2.6.2.4.8. Gerenciamento de chaves de licença.

2.2.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

2.2.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

2.2.6.2.6. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede.

2.2.6.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros etc.).

2.2.6.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS).

2.2.6.2.9. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares.

2.2.6.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

2.2.6.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.

2.2.6.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

2.2.6.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

2.2.6.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex:

"Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.2.6.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.2.6.2.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.2.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

2.2.6.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (exemplo: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários etc.).

2.2.6.2.19. Capacidade de verificar objetos usando heurística.

2.2.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

2.2.6.2.21. Capacidade de agendar uma pausa na verificação.

2.2.6.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

2.2.6.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.2.6.2.23.1. Perguntar o que fazer, ou;

2.2.6.2.23.2. Bloquear acesso ao objeto.

2.2.6.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.6.2.23.2.2. Caso positivo de desinfecção:

2.2.6.2.23.2.2.1. Restaurar o objeto para uso.

2.2.6.2.23.3. Caso negativo de desinfecção:

2.2.6.2.23.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.6.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.2.6.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.2.6.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

2.2.6.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

2.2.6.2.28. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

2.2.6.2.29. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.2.6.2.30. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

2.2.7. Servidores Linux

2.2.7.1. Compatibilidade:

2.2.7.1.1. Plataforma 32 bits:

2.2.7.1.1.1. Ubuntu 16.04 LTS.

2.2.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

2.2.7.1.1.3. CentOS-6.7.

2.2.7.1.1.4. Debian GNU / Linux 9.4.

2.2.7.1.2. Plataforma 64 bits:

2.2.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

2.2.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

2.2.7.1.2.3. CentOS-6.7, 7.2, 8.0.

2.2.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

2.2.7.1.2.5. OracleLinux 7.3, 8.

2.2.7.1.2.6. SUSE® Linux Enterprise Server 15.

2.2.7.1.2.7. openSUSE® 15.

2.2.7.1.2.8. Amazon Linux AMI.

2.2.7.2. Características:

2.2.7.2.1. Deve prover as seguintes proteções:

2.2.7.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

2.2.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

2.2.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

2.2.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

2.2.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

2.2.7.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.2.7.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.2.7.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.2.7.2.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

2.2.7.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

2.2.7.2.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

2.2.7.2.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

2.2.7.2.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.2.7.2.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.2.7.2.7. Capacidade de verificar objetos usando heurística.

2.2.7.2.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.2.7.2.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

2.2.7.2.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

2.2.8. Smartphones e tablets

2.2.8.1. Compatibilidade:

2.2.8.1.1. Dispositivos com os sistemas operacionais:

2.2.8.1.1.1. Android 4.2 – 11.

2.2.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

2.2.8.2. Características:

2.2.8.2.1. Deve prover as seguintes proteções:

2.2.8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

2.2.8.2.1.2. Proteção contra adware e autodialers.

2.2.8.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.

2.2.8.2.1.4. Arquivos abertos no smartphone.

2.2.8.2.1.5. Programas instalados usando a interface do smartphone

2.2.8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento.

2.2.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

2.2.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

2.2.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

2.2.8.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.

2.2.8.2.6. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha.

2.2.8.2.7. Deverá ter firewall pessoal (Android).

2.2.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

2.2.8.2.9. Capacidade de enviar comandos remotamente de:

2.2.8.2.9.1. Localizar.

2.2.8.2.9.2. Bloquear.

2.2.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

2.2.8.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos.

2.2.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

2.2.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

2.2.8.2.14. Capacidade de localizar o dispositivo quando necessário.

2.2.8.2.15. Permitir atualização das definições quando estiver em "roaming".

2.2.8.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus.

2.2.8.2.17. Deve permitir verificar somente arquivos executáveis.

2.2.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

2.2.8.2.19. Capacidade de agendar uma verificação.

2.2.8.2.20. Capacidade de enviar URL de instalação por e-mail.

2.2.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

2.2.8.2.22. Capacidade de executar as seguintes ações caso a desinfecção falhe:

2.2.8.2.22.1. Deletar.

2.2.8.2.22.2. Ignorar.

2.2.8.2.22.3. Quarentenar.

2.2.8.2.22.4. Perguntar ao usuário.

2.2.9. Gerenciamento de dispositivos móveis (MDM):

2.2.9.1. Compatibilidade:

2.2.9.1.1. Android 4.2 – 11.

2.2.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

2.2.9.2. Características:

2.2.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

2.2.9.2.2. Capacidade de ajustar as configurações de:

2.2.9.2.2.1. Sincronização de e-mail.

2.2.9.2.2..2. Uso de aplicativos.

2.2.9.2.2.3. Senha do usuário.

2.2.9.2.2.4. Criptografia de dados.

2.2.9.2.2.5. Conexão de mídia removível.

2.2.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

2.2.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

2.2.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

2.2.9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS.

2.2.9.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento.

2.2.9.2.8. Permitir sincronização com perfil do "Touch Down".

2.2.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

2.2.9.2.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual.

2.2.9.2.11. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

2.3. Transferência de conhecimento e direitos de propriedade intelectual

2.3.1. O uso de uma solução de antivírus corporativo é imprescindível por conter funções de proteção que vão além de um antivírus comum, evitando, portanto, invasões ou roubos de informações, por exemplo. Por isso, não existe versões corporativas gratuitas, não sendo vislumbrada outra forma de utilização senão a obrigatoriedade da renovação/aquisição dessa tecnologia de terceiros.

2.3.2. Os antivírus corporativos são produtos consolidados no mercado de Tecnologia da Informação e Comunicação no Brasil e utilizados por organizações públicas e privadas. Desta forma, os riscos de descontinuidade desse produto no mercado parecem ser mínimos.

2.3.3. A Contratada deverá realizar a transferência de conhecimento nas versões dos softwares que serão adquiridos pelo Contratante e com isso, repassar informações de configuração, testes, procedimentos de contingência e demais informações necessárias para a operação e manutenção da solução.

2.3.4. Não se aplica o requisito pertinente aos direitos de propriedade intelectual e autoral da STIC, uma vez que não será produzido nenhum artefato, tampouco trata de desenvolvimento de software.

3. GARANTIA E SUPORTE

3.1. Garantia

3.1.1. Durante o período de vigência do contrato a garantia se dará em forma de suporte técnico e seguirá as especificações descritas no Termo de Referência que tratarão as respostas a incidentes de segurança.

3.1.2. A Contratada deverá prestar garantia, com o fornecimento de novas versões, pelo período de 36 (trinta e seis) meses, contados a partir da assinatura do Termo de Recebimento Definitivo.

3.1.3. Incluem-se, na garantia, os serviços de manutenção, suporte técnico, atualização de software e produto, bem como o auxílio na utilização de recursos ou solução de problemas relacionados aos softwares ofertados.

3.2. Suporte Técnico

3.2.1. Durante a vigência do contrato deverá ser fornecido suporte técnico pela Contratada seguindo as especificações abaixo:

3.2.1.1. Apoio às respostas a incidentes de segurança envolvendo malware.

3.2.1.2. Suporte técnico para eventuais dúvidas ou problemas com a solução.

3.2.1.3. Acompanhamento nos chamados escalados para o Fabricante em situações de falhas/problemas desconhecidos pelo suporte técnico da Contratada ou bugs.

3.2.1.4. O atendimento deverá ser realizado via contato telefônico ou ferramenta de acesso remoto independentemente do tipo de incidente.

3.2.1.5. Suporte técnico 8x5, prestado unicamente à equipe de segurança da área de tecnologia do Contratante, referente a problemas de funcionamento/configuração dos produtos fornecidos.

3.2.1.6. Número de chamados ilimitados;

3.2.2. Incidentes, chamados, e problemas escalados ao Fabricante deverão atender os prazos estabelecidos na tabela abaixo:

Níveis de Severidade	Descrição	Prazo para solução
Nível 1 – Crítico	Afeta o serviço prestado pelo Contratante por interrupções da solução de antivírus nos sistemas operacionais, possíveis perda de dados, alterações de configuração padrão para configuração insegura e onde não há solução alternativa disponível.	6 horas
Nível 2 – Alto	Afeta a funcionalidade do produto, mas não causa corrupção e perda de dados ou travamento sistemas.	10 horas
Nível 3 – Médio	Solicitações não críticas, as quais não afetam a funcionalidade do produto.	12 horas
Nível 4 – Baixo	Solicitações não críticas ou solicitação de serviços. Todos os incidentes que não satisfaçam um dos critérios listados acima, serão classificados a esse nível de gravidade.	14 horas

3.2.3. Será respeitado o horário de expediente do Contratante, caso o prazo de solução expire em horário não comercial, a contagem do prazo de solução será paralisada no final do expediente e iniciada no próximo dia útil, contando o prazo de solução já decorrido do chamando no dia anterior.

3.2.4. A Contratada deverá prestar suporte técnico e operacional durante o período de vigência da licença, com atendimento através do serviço telefônico (0800), acesso remoto, e-mail ou WEB, para esclarecimento de dúvidas, abertura de chamados, e envio de arquivos para análise.

3.2.5. Ambos os objetos 1) Renovação de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select; e 2) Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select deverão ser atendidos com essas exigências de suporte técnico.

4. GESTÃO E FISCALIZAÇÃO CONTRATUAL

4.1. Profissionais da Contratada: equipe composta por técnicos da Contratada, responsáveis pela execução e acompanhamento do objeto.

4.1.1. Técnico: funcionário da Contratada, responsável pela execução técnica-operacional.

4.1.2. Preposto: funcionário representante da Contratada, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

4.2. Equipe de Gestão do Contrato: equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares.

4.2.1. Gestor do Contrato: servidor responsável pela gestão contratual, conforme Decreto Judiciário nº 291, de 2009 e Portaria nº 255, de 2009, do Tribunal de Justiça do Estado do Tocantins.

4.2.2. Fiscal Demandante: servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos funcionais da solução.

4.2.3. Fiscal Técnico: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.

4.2.4. Fiscal Administrativo: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

4.3. A atuação ou a eventual omissão da Fiscalização durante a realização dos trabalhos, não poderá ser invocada para eximir a Contratada da responsabilidade no fornecimento dos produtos.

4.4. A fiscalização será sob o aspecto qualitativo e quantitativo, devendo ser anotado, em registro próprio as falhas detectadas, e comunicadas ao gestor do contrato todas as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por

parte da Contratada.

4.5. A comunicação entre a fiscalização e a Contratada será realizada por meio de correspondência oficial e anotações ou registros no mesmo processo que tratam da aquisição dos objetos.

4.6. Quando houver necessidade o gestor deverá emitir notificações para a Contratada.

5. DINÂMICA DE EXECUÇÃO

5.1. A tabela abaixo sintetiza as etapas de execução desta contratação. O prazo em todas as etapas tem como referência inicial o fim da etapa anterior.

Etapa	Descrição	Quando ocorre
1	Recebimento do pedido de fornecimento.	O TJTO encaminhará o pedido de fornecimento a qualquer tempo dentro da vigência da Ata de Registro de Preços e após a assinatura do contrato.
2	Entrega das licenças.	O prazo será de até 20 (vinte) dias úteis, contados a partir da data de assinatura do contrato ou recebimento da nota de empenho.
3	Recebimento provisório das licenças.	Imediatamente após o recebimento das licenças, para efeito de posterior verificação da conformidade do material com a especificação, nos termos do artigo 73, da Lei nº 8.666, de 1993.
4	Avaliação das licenças entregues.	Após a entrega, será realizada uma avaliação e homologação pelos responsáveis técnicos. A análise para comprovação das características técnicas consistirá em avaliar as documentações apresentadas e também informações de registro das licenças no site oficial do fabricante.
5	Recebimento Definitivo das licenças.	O responsável técnico deverá, após a comprovação do atendimento das especificações técnicas, emitir e assinar em, no máximo, 15 (quinze) dias úteis, contados do primeiro dia útil posterior à entrega dos equipamentos, o Termo de Recebimento Definitivo, nos termos do artigo 73, da Lei nº 8.666, de 1993.
6	Início da contagem do prazo de garantia.	Data da emissão do recebimento definitivo das licenças. Se for o caso de licenças vincendas, a garantia iniciará no dia subsequente após o fim da vigência desta.
7	Fim do prazo de garantia	Após 36 (trinta e seis) meses.

6. DO RECEBIMENTO

6.1. O Tribunal de Justiça expedirá "Termo de Recebimento Provisório", o qual deverá ser assinado pelo gestor, para efeito de posterior verificação da conformidade dos objetos com as especificações constantes neste Termo de Referência, nos termos do artigo 73, da Lei nº 8.666, de 1993.

6.2. Após a verificação da qualidade e quantidade do material e consequente aceitação, nos termos do artigo 73, da Lei nº 8.666, de 1993, o Tribunal de Justiça emitirá "Termo de Recebimento Definitivo", no prazo de 15 (quinze) dias, o qual deverá ser assinado pelo gestor.

6.3. O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com este termo de referência.

6.4. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato.

6.5. O Fornecedor é obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

7. DO PAGAMENTO

7.1. O Fornecedor deverá apresentar nota fiscal, correspondente aos produtos efetivamente entregues.

7.2. O Contratante reserva-se o direito de não realizar o atesto, se os dados estiverem em desacordo com os dados do Fornecedor ou, ainda, se o objeto entregue não estiver em conformidade com as especificações apresentadas neste Termo de Referência, ficando o pagamento suspenso até a regularização.

7.3. O atesto do gestor é condição indispensável para o pagamento.

7.4. Na ausência do fiscal do contrato (férias, licença ou em viagem por interesse do Poder Judiciário), o atesto será dado pelo gestor substituto.

7.5. O pagamento será efetuado em até 30 (trinta) dias corridos, contados a partir do protocolo de recebimento da nota fiscal, sendo que, recaindo sobre dias não úteis, o termo final será prorrogado para o dia útil subsequente.

7.6. O CNPJ deverá ser o mesmo indicado na proposta, nota de empenho e vinculado à conta corrente do Fornecedor.

7.7. Todos os atos inerentes ao presente processo obedecerão às regras concernentes ao Sistema de Eletrônico de Informação do Tribunal de Justiça do Estado do Tocantins – SEI.

8. DA ATA DE REGISTRO DE PREÇOS

8.1. A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da sua publicação.

9. DO CONTRATO

9.1. Caso exista demanda dos objetos registrados e havendo orçamento para realizar a contratação, o Tribunal de Justiça do Estado do Tocantins firmará contrato para adquiri-los nos quantitativos necessários para suprir suas necessidades.

9.2. No ato de assinatura do contrato, a Contratada deverá atender as disposições da Portaria nº 97, de 2010, quanto à verificação da regularidade fiscal. Se qualquer das certidões apresentadas na fase de habilitação do procedimento licitatório expirar sua validade antes da data de assinatura dos contratos ou de seus aditivos, deverá ser atualizada.

9.3. Os contratos a serem firmados terão vigência de 36 (trinta e seis) meses, contados a partir do recebimento definitivo da solução adquirida.

10. SANÇÕES ADMINISTRATIVAS

10.1. A empresa que, convocada dentro do prazo de validade da sua proposta, não celebrar o contrato, quando exigido, deixar de entregar a documentação exigida para o certame ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedida de licitar e contratar com a Administração Pública do Estado do Tocantins e será descredenciada no Sistema de Cadastramento Unificado de Fornecedores (Sicaf), pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e das demais cominações legais.

10.2. Subsidiariamente, nos termos do artigo 87, da Lei nº 8.666, de 1993, pela inexecução total ou parcial das condições estabelecidas neste instrumento, o Poder Judiciário do Estado do Tocantins poderá, garantida a prévia defesa da empresa, que deverá ser apresentada no prazo de 5 (cinco) dias úteis a contar da sua notificação, aplicar, sem prejuízo das responsabilidades penal e civil, as seguintes sanções:

10.2.1. Advertência, por escrito, quando a empresa deixar de atender quaisquer indicações aqui constantes;

10.2.2. Multa compensatória/indenizatória no percentual de 5% (cinco por cento) calculado sobre o valor contratado;

10.2.3. Suspensão temporária de participação em licitação e impedimento de contratar com o Poder Judiciário do Estado do Tocantins, pelo prazo de até 2 (dois) anos; e

10.2.4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

10.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pela empresa, a esta será aplicada multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor do contrato ou instrumento equivalente, por dia de atraso, limitada a 10% (dez por cento) do valor inadimplido.

10.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhido ao Fundo Especial de Modernização e Aprimoramento do Poder Judiciário – FUNJURIS, dentro do prazo de 5 (cinco) dias úteis após a respectiva notificação.

10.5. Caso não seja paga no prazo previsto no subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado pelo Poder Judiciário do Estado do Tocantins ou cobrada judicialmente.

10.6. Além das penalidades citadas, a empresa ficará sujeita, ainda, no que couber, às demais penalidades previstas em lei.

11. FUNDAMENTAÇÃO DA CONTRATAÇÃO

11.1. Justificativa e motivação

11.1.1. O Poder Judiciário do Estado do Tocantins, por meio da Diretoria de Tecnologia da Informação, tem se empenhado no planejamento para a sustentação técnica do ambiente de Tecnologia da Informação e Comunicação e contratação dos serviços e produtos relacionados. Com base nisso, essa contratação visa adquirir licença de solução de antivírus corporativo.

11.1.2. A existência de ataques de vírus dentro da Rede deste Poder Judiciário pode causar riscos às informações e atraso na execução de tarefas devido a problemas, tais como: lentidão, perda de arquivos importantes, parada de sistemas e até a exploração de informações sigilosas.

11.1.3. O Poder Judiciário utiliza a solução de antivírus Kaspersky Endpoint Security, instalada, configurada e operante em todo seu parque tecnológico, com equipe técnica devidamente capacitada para administrar a referida solução.

11.1.4. A renovação/aquisição do antivírus, justifica-se por ser essencial para viabilizar a proteção adequada e atualizada no ambiente computacional deste Poder Judiciário, permitindo preservar os ativos corporativos (hardware, software e, sobretudo, dados), garantindo a integridade, confiabilidade e segurança, além da continuidade das atividades da organização.

11.1.5. Atualmente este Poder Judiciário dispõe de 2.000 licenças, do Contrato nº 99/2018 e 850 licenças, do Contrato nº 128/2019, que irão expirar nos meses de setembro e novembro de 2021, respectivamente. Vale destacar que uma mudança para outro software de antivírus ocasionaria um gasto desnecessário de tempo e custos, visto que necessitaria de uma nova implantação – incluindo custos com viagens (diárias) para instalar em equipamentos no interior, por exemplo, e nova capacitação para o corpo técnico em se tratando de solução distinta.

11.1.6. Ademais, a atual solução tem atendido às necessidades deste Poder Judiciário de forma satisfatória, não registrando, até então, incidentes relevantes durante o tempo de uso da solução.

11.1.7. Por se tratar de solução imprescindível para a segurança da informação na instituição, faz-se necessária a manutenção do software sob contrato de prestação de serviço de suporte técnico e de garantia de atualização de versão.

11.1.8. O emprego desta ferramenta de segurança possibilita monitorar e controlar o tráfego de dados que circula entre as redes internas e a Internet, garantindo a segurança e o bom funcionamento dos computadores da rede local (Intranet) contra ações de vírus e, ainda, permite a implantação de uma política de prevenção de riscos.

11.1.9. Faz-se necessária, portanto, a renovação de licenças do antivírus Kaspersky Endpoint Security – Versão Business Select – pelo período de 36 (trinta e seis) meses, para prevenir a ocorrência dos eventos citados e com isso, assegurar a continuidade dos serviços prestados, uma vez que a contratação de 2.000 licenças, do Contrato nº 99/2018 e 850 licenças, do Contrato nº 128/2019, irão expirar nos meses de setembro e novembro, respectivamente. Outrossim, vislumbramos a necessidade de registrar ata para 650 licenças as quais permitirão suprir futura demanda com aumento de computadores no parque tecnológico deste Judiciário.

11.2. Objetivos e benefícios

11.2.1. Prevenir ataques de vírus e outras ameaças digitais dentro da rede deste Poder Judiciário que possam causar perda de arquivos importantes e exploração de informações sigilosas.

11.2.2. Monitorar e controlar o tráfego de dados que circulam entre as redes interna e a Internet.

11.2.3. Garantir o bom funcionamento dos computadores da rede local contra ação de vírus.

11.2.4. Garantir acesso seguro às informações armazenadas nas bases de dados do Judiciário tocantinense.

11.2.5. Administrar os computadores da rede aplicando-lhes políticas de segurança remotamente.

11.2.6. Permitir a melhoria constante da infraestrutura e governança de TIC.

11.3. Alinhamento estratégico

11.3.1. A aquisição Solução de Tecnologia da Informação e Comunicação está contemplada no Plano de Contratação de 2021 da Diretoria de Tecnologia da Informação, conforme se depreende do SEI nº 19.0.000003602-4, evento 3492556, descrita como "Licenças Antivírus" – item 45.

11.3.2. O objeto da contratação está alinhado com um dos objetivos estratégicos definidos na Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça, qual seja:

11.3.3. Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados.

11.4. Referência aos estudos preliminares

11.4.1. Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda (DOD) e Estudos Preliminares, insertos nos eventos 3546947 e 3575158, respectivamente, do processo SEI nº 21.0.000002638-4.

11.5. Relação entre a Demanda Prevista e a Contratada

11.5.1. Atualmente, há cerca de 3.055 computadores (entre desktops e notebooks) distribuídos entre Tribunal de Justiça, Comarcas, Juizados e Anexos já com a solução de segurança instalada e operante.

11.5.2. A demanda prevista consiste na renovação de 2.850 licenças que terão sua vigência expirada, sendo que outras 650 licenças excedentes visam garantir o crescimento do parque tecnológico.

11.6. Análise de Mercado de TIC

11.6.1. Atualmente existem no mercado vários fabricantes de antivírus, sendo diferenciados pela eficiência quanto à proteção. No mercado de antivírus corporativo, pode-se citar os seguintes fabricantes: Avira, Symantec, Kaspersky, McAfee, Panda, BitDefender, Trendmicro, Sophos, Eset, entre outros.

11.6.2. Também foi realizada uma pesquisa acerca de contratações similares realizadas por outras pessoas jurídicas de direito público com a finalidade de identificação de soluções semelhantes à desejada pelo Contratante.

11.6.3. Foram algumas pessoas jurídicas que buscaram realizar licitação cujo objeto é solução de antivírus: Tribunal de Justiça do Estado de Mato Grosso; Seção Judiciária do Rio Grande do Sul (TRF4); Secretaria da Fazenda e Planejamento do Estado do Tocantins; Defensoria Pública do Estado de Goiás; Governo do Estado do Ceará; Universidade Federal do Goiás; Prefeitura Municipal de Anchieta-ES.

11.7. Natureza do objeto

11.7.1. O objeto possui natureza de bem de consumo, pois se trata de licença de antivírus. É salutar que o objeto possui características comuns e usuais encontrados no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos.

11.8. Parcelamento e Adjudicação do objeto

11.8.1. No contexto desta contratação e de acordo com os requisitos levantados, verifica-se que o objeto é composto por itens, sendo um item para renovação das licenças e outro para aquisição de licenças.

11.8.2. Observa-se que a adjudicação pode ser realizada a fornecedores diversos, não havendo problema se for adjudicado a único fornecedor.

11.9. Modalidade, Tipo de Licitação e Critérios de Seleção

11.9.1. Verifica-se que o objeto pretendido é oferecido por diversos fornecedores no mercado de TIC e apresentam características padronizadas e usuais. Assim, pode-se concluir que o objeto é comum e, portanto, sugere-se como melhor opção a utilização da modalidade "Pregão".

11.9.2. As licenças de solução corporativa de antivírus têm papel essencial à continuidade das atividades deste Poder Judiciário de forma segura, será exigido atestado de capacidade técnica, nos termos da Instrução Normativa nº 9, de 20 de julho de 2018, do Tribunal de Justiça do Estado do Tocantins, uma vez que a não comprovação pode implicar na insatisfação na execução da dos serviços prestado.

11.9.3. Igualmente, o critério de habilitação busca filtrar as empresas que realmente pertencem à área de tecnologia da informação e comunicação, ou seja, do ramo do objeto que se pretende contratar, de modo a minimizar riscos para a regular execução do objeto.

11.9.4. Portanto, o atestado de capacidade técnica, quando solicitado pela Administração nas contratações realizadas pelo Poder Judiciário do Estado do Tocantins:

11.9.4.1. Poderá ser emitido por pessoa jurídica de direito público ou privado.

11.9.4.2. Terá a finalidade de comprovar que o licitante forneceu ou está fornecendo objetos e/ou prestou ou está prestando serviços satisfatoriamente, de forma compatível com o objeto da contratação.

11.9.4.3. O atestado emitido por pessoa jurídica de direito privado será assinado pelo representante legal da pessoa emitente, o qual se responsabilizará na forma da lei.

11.9.4.4. Deverá constar no atestado, no mínimo, os seguintes dados do emitente: razão social e dados para contato; e do favorecido: razão social, número do CNPJ, objeto do contrato e dados para contato.

11.9.4.5. Será admitida a somatória de atestados de capacidade técnica sempre que inexistir motivo para a exigência de atestado único, independente da época de expedição ou localidade.

11.9.4.6. Será facultada à Comissão de Licitação, ao Pregoeiro ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo, vedada a inclusão posterior de documento ou informação relevante que deveria constar originariamente da proposta.

11.10. Impacto ambiental

11.10.1. A solução de TIC que se pretende contratar diz respeito a renovação/aquisição de licenças de antivírus e se trata de um software. Neste caso não ocorrerá descarte de nenhum equipamento, com isso, não haverá impacto ao ambiente.

11.11. Conformidade Técnica e Legal

11.11.1. A contratação deve estar de acordo com a: Lei nº 8.666, de 21 de junho de 1993; Decreto nº 10.024, de 20 de setembro de 2019; e Resolução CNJ de nº 370, de 28 de janeiro de 2021.

11.12. Obrigações Contratuais

11.12.1. Da Contratada

11.12.1.1. Responsabilizar-se pela observância de Leis, Decretos, Regulamentos, Portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto do contrato, bem como, aplicáveis aos casos de subcontratação.

11.12.1.2. Atender prontamente às solicitações do Tribunal de Justiça do Estado do Tocantins no fornecimento do objeto nas quantidades e especificações deste Termo de Referência, de acordo com a necessidade desta Corte, a partir da solicitação do gestor do contrato.

11.12.1.3. Manter, durante a execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação, em conformidade com a Lei, incluindo a atualização de documentos de controle da arrecadação de tributos e contribuições federais e outras legalmente exigíveis.

11.12.1.4. Responsabilizar-se por todos os recursos e insumos necessários ao perfeito cumprimento do objeto contratado, devendo estar incluídas no preço proposto todas as despesas com materiais, insumos, seguros, impostos, taxas, encargos e demais despesas necessárias à perfeita execução do objeto.

11.12.1.5. Indicar, formalmente, preposto apto a representá-la junto ao Contratante, que deverá responder pela fiel execução do contrato.

11.12.1.6. Prestar todos os esclarecimentos técnicos que lhe forem solicitados pelo Contratante, relacionados com as características e funcionamento do objeto, inclusive em relação aos problemas detectados.

11.12.1.7. Comunicar, imediatamente, por escrito qualquer anormalidade, prestando ao Contratante os esclarecimentos julgados necessários.

11.12.1.8. Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados; treinados e qualificados para prestação dos serviços.

11.12.1.9. Manter ficha de controle do serviço, na qual serão relatadas todas as ocorrências.

11.12.1.10. Assumir inteira responsabilidade técnica e operacional, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas na prestação do objeto.

11.12.1.11. Ficar obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nas aquisições até 25% (vinte e cinco por cento) do valor inicial deste Termo de Referência, nos termos da Lei.

11.12.1.12. Não transferir a outrem, no todo ou em parte, o objeto desta prestação.

11.12.1.13. Identificar qualquer equipamento de sua posse que venha a ser utilizado nas dependências do Poder Judiciário, afixando placas de controle patrimonial, selos de segurança etc.

11.12.1.14. Reparar quaisquer danos diretamente causados ao Contratante ou a terceiros, por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da presente relação contratual, não excluindo ou reduzindo essa responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pelo Contratante.

11.12.1.15. Cumprir integralmente as exigências do Acordo de Nível de Serviço, disposto no "ANEXO C" deste Termo de Referência.

11.12.1.16. Manter sigilo sobre todo e qualquer assunto de interesse do Poder Judiciário ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa.

11.12.2. Do Contratante

11.12.2.1. Responsabilizar-se pela observância às Leis, Decretos, Regulamentos, Portarias e demais normas legais, direta e indiretamente aplicáveis ao contrato.

11.12.2.2. Receber o objeto de acordo com as disposições deste Termo de Referência.

11.12.2.3. Comunicar imediatamente a Contratada qualquer incorreção apresentada com o objeto entregue.

11.12.2.4. Acompanhar e fiscalizar a execução do Contrato.

11.12.2.5. Responsabilizar-se pela lavratura do respectivo contrato, com base nas disposições da Lei.

11.12.2.6. Assegurar os recursos orçamentários e financeiros para custear os bens adquiridos e promover os pagamentos dentro dos prazos convencionados neste Termo de Referência.

11.12.2.7. Processar e liquidar a fatura correspondente aos valores, através de Ordem Bancária.

11.12.2.8. Zelar para que durante a vigência do contrato sejam cumpridas as obrigações assumidas por parte da Contratada, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas.

12. DISPOSIÇÕES GERAIS

12.1. A proposta deverá conter as especificações do objeto de forma clara, descrevendo detalhadamente as características técnicas do produto ofertado, incluindo especificação, marca, modelo, garantia, procedência e outros elementos que de forma inequívoca identifiquem e constatem as configurações cotadas.

ANEXO "A" DO TERMO DE REFERÊNCIA

MINUTA DO TERMO DE RECEBIMENTO PROVISÓRIO DE BENS NÃO PERMANENTES

Aos _____ dias do mês de _____ do ano de _____, este(a) GESTOR(A) encerrou os trabalhos de análise para fim de RECEBIMENTO PROVISÓRIO, previsto no Contrato nº _____/_____ (ou Nota de Empenho nº _____/_____), do Processo nº _____. Assim procedendo, este Gestor conferiu o objeto apresentado e atesta o RECEBIMENTO PROVISÓRIO, sem (ou com as seguintes) ressalvas:

1. (listar as discrepâncias, quando houver)

Palmas, _____ de _____ de _____.

_____
Gestor(a)

ANEXO "B" DO TERMO DE REFERÊNCIA

MINUTA DO TERMO DE RECEBIMENTO DEFINITIVO DE BENS NÃO PERMANENTES

Aos _____ dias do mês de _____ do ano de _____, este(a) GESTOR(A), declara para os devidos fins, que recebe definitivamente, o objeto apresentado e atesta o RECEBIMENTO DEFINITIVO, do objeto previsto no Contrato nº _____/_____ (ou Nota de Empenho nº _____/_____), do Processo nº _____.

Palmas, _____ de _____ de _____.

_____
Gestor(a)

ANEXO "C" DO TERMO DE REFERÊNCIA

ACORDO DE NÍVEL DE SERVIÇO

1. Acordo de Nível de Serviço para entrega dos objetos:

Ação	Descrição	Medidas corretivas
Prazo para entrega do objeto	Até 1 (um) dia útil de atraso referente ao prazo do tópico 5.1 deste Termo de Referência.	Advertência.
	Superior a 1 (um) útil dia e inferior a 4 (quatro) dias úteis de atraso referente ao prazo do tópico 5.1 deste Termo de Referência.	Glosa de 0,1% (zero vírgula um por cento) sobre o valor total do Contrato por dia de atraso.
	A partir de 4 (quatro) dias úteis de atraso referente ao prazo do tópico 5.1 deste Termo de Referência.	Glosa de 0,1% (zero vírgula um por cento) ao dia de atraso sobre o valor total do Contrato.
Prazo para solução de problema	Até 2 (duas) horas de atraso referente aos prazos dos tópicos 3.2.2 deste Termo de Referência.	Advertência.
	Superior a 2 (duas) horas de atraso referente aos prazos dos tópicos 3.2.2 deste Termo de Referência.	Glosa de 0,05% (zero vírgula zero cinco por cento) à hora de atraso sobre o valor do contrato.
Enviar empregado sem qualificação para executar os serviços contratados.		Glosa de 0,1% (zero vírgula um por cento) por ocorrência, contada a partir da terceira eventualidade, sobre o valor total do contrato.
Deixar de cumprir determinação formal ou instrução complementar do órgão fiscalizador.		Glosa de 0,3% (zero vírgula três por cento) por ocorrência.

2. É garantido à Contratada o direito de contestação dos resultados da apuração do Acordo de Nível de Serviço, bem como apresentar as justificativas que se fizerem necessárias.

3. As justificativas, desde que aceitas pelo gestor e pelo fiscal do contrato, poderão anular a incidência de glosas e advertências na aplicação do Acordo de Nível de Serviço.

4. As penalidades deste item não excluem, nem alteram as especificadas nas Sanções Administrativas.

Termo de Referência Nº 192 / 2021 - PRESIDÊNCIA/DIGER/DTINF/GABDTI

1. OBJETO

1.1. Visa o presente Termo de Referência registrar preços, objetivando a renovação e a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – Versão Business Select, incluindo atualizações e suporte técnico pelo período de 36 (trinta e seis) meses, para atender as demandas do Poder Judiciário do Estado do Tocantins, conforme as especificações e quantidades estabelecidas neste documento, mediante licitação regida pelo Decreto Judiciário nº 6 de 14 de janeiro de 2020.

Item	Descrição	CATMAT / CATSER	Unidade	Qtde.	Valor Estimado Unitário	Total
1	Renovação de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select.	350949	Un.	2.850	R$ 113,19	R$ 322.591,50
	Aquisição de licenças do software de					

2	antivírus Kaspersky Endpoint Security – Versão Business Select.	350949	Un.	650	R$ 117,20	R$ 76.180,00
Total Geral						R$ 398.771,50

2. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

2.1. Renovação de licenças de solução corporativa de antivírus

2.1.1. Características Gerais

2.1.1.1. Todas as licenças fornecidas terão validade de 36 (trinta e seis) meses para atualizações inerentes ao produto.

2.1.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

2.1.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

2.1.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para o Contratante além daquele já cotado na proposta.

2.1.2. Servidor de Administração e Console Administrativa

2.1.2.1. Compatibilidade:

2.1.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

2.1.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

2.1.2.1.3. Microsoft Windows Server 2016 x64.

2.1.2.1.4. Microsoft Windows Server 2019 x64.

2.1.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

2.1.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

2.1.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

2.1.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

2.1.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

2.1.2.2. Características:

2.1.2.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC.

2.1.2.2.2. Console deve ser baseada no modelo cliente/servidor.

2.1.2.2.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.

2.1.2.2.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.

2.1.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

2.1.2.2.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM.

2.1.2.2.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores.

2.1.2.2.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory.

2.1.2.2.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.

2.1.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

2.1.2.2.11. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada.

2.1.2.2.12. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas.

2.1.2.2.13. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas.

2.1.2.2.14. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador.

2.1.2.2.15. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle.

2.1.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

2.1.2.2.17. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus.

2.1.2.2.18. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança.

2.1.2.2.19. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede.

2.1.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

2.1.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

2.1.2.2.22. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes.

2.1.2.2.23. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

2.1.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

2.1.2.2.25. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

2.1.2.2.25.1. Nome do computador.

2.1.2.2.25.2. Nome do domínio.

2.1.2.2.25.3. Range de IP.

2.1.2.2.25.4. Sistema Operacional.

2.1.2.2.25.5. Máquina virtual.

2.1.2.2.26. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas.

2.1.2.2.27. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional.

2.1.2.2.28. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção.

2.1.2.2.29. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção.

2.1.2.2.30. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente.

2.1.2.2.31. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias etc.

2.1.2.2.32. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos.

2.1.2.2.33. Deve fornecer as seguintes informações dos computadores:

2.1.2.2.33.1. Se o antivírus está instalado.

2.1.2.2.33.2. Se o antivírus está iniciado.

2.1.2.2.33.3. Se o antivírus está atualizado.

2.1.2.2.33.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo.

2.1.2.2.33.5. Minutos/horas desde a última atualização de vacinas.

2.1.2.2.33.6. Data e horário da última verificação executada na máquina.

2.1.2.2.33.7. Versão do antivírus instalado na máquina.

2.1.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças.

2.1.2.2.33.9. Data e horário de quando a máquina foi ligada.

2.1.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina.

2.1.2.2.33.11. Nome do computador.

2.1.2.2.33.12. Domínio ou grupo de trabalho do computador.

2.1.2.2.33.13. Data e horário da última atualização de vacinas.

2.1.2.2.33.14. Sistema operacional com Service Pack.

2.1.2.2.33.15. Quantidade de processadores.

2.1.2.2.33.16. Quantidade de memória RAM.

2.1.2.2.33.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory).

2.1.2.2.33.18. Endereço IP.

2.1.2.2.33.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.

2.1.2.2.33.20. Atualizações do Windows Updates instaladas.

2.1.2.2.33.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD.

2.1.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina.

2.1.2.2.34. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las.

2.1.2.2.35. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

2.1.2.2.35.1. Alteração de Gateway Padrão.

2.1.2.2.35.2. Alteração de subrede.

2.1.2.2.35.3. Alteração de domínio.

2.1.2.2.35.4. Alteração de servidor DHCP.

2.1.2.2.35.5. Alteração de servidor DNS.

2.1.2.2.35.6. Alteração de servidor WINS.

2.1.2.2.35.7. Alteração de subrede.

2.1.2.2.35.8. Resolução de Nome.

2.1.2.2.35.9. Disponibilidade de endereço de conexão SSL.

2.1.2.2.36. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet.

2.1.2.2.37. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes.

2.1.2.2.38. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus.

2.1.2.2.39. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos.

2.1.2.2.40. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede.

2.1.2.2.41. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.

2.1.2.2.42. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

2.1.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos.

2.1.2.2.44. Capacidade de enviar e-mails para contas específicas em caso de algum evento.

2.1.2.2.45. Listar em um único local, todos os computadores não gerenciados na rede.

2.1.2.2.46. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes.

2.1.2.2.47. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

2.1.2.2.48. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação etc.), inclusive de máquinas que estejam em subnets diferentes do servidor.

2.1.2.2.49. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo).

2.1.2.2.50. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador.

2.1.2.2.51. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (exemplo: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint).

2.1.2.2.52. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação.

2.1.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

2.1.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

2.1.2.2.55. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

2.1.2.2.55.1. Nome do vírus.

2.1.2.2.55.2. Nome do arquivo infectado.

2.1.2.2.55.3. Data e hora da detecção.

2.1.2.2.55.4. Nome da máquina ou endereço IP.

2.1.2.2.55.5. Ação realizada.

2.1.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

2.1.2.2.57. Capacidade de listar updates nas máquinas com o respectivo link para download.

2.1.2.2.58. Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração.

2.1.2.2.59. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante.

2.1.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente.

2.1.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2.1.3. Estações Windows

2.1.3.1. Compatibilidade:

2.1.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate.

2.1.3.1.2. Microsoft Windows 8 Professional/Enterprise.

2.1.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

2.1.3.1.4. Microsoft Windows 10 Professional/Enterprise.

2.1.3.2. Características:

2.1.3.2.1. Deve prover as seguintes proteções:

2.1.3.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.1.3.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus).

2.1.3.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos).

2.1.3.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza.

2.1.3.2.1.5. Firewall com IDS.

2.1.3.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus).

2.1.3.2.1.7. Controle de dispositivos externos.

2.1.3.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

2.1.3.2.1.9. Controle de acesso a sites por horário.

2.1.3.2.1.10. Controle de acesso a sites por usuários.

2.1.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

2.1.3.2.1.12. Controle de execução de aplicativos.

2.1.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

2.1.3.2.2.Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.1.3.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

2.1.3.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

2.1.3.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (exemplo: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.1.3.2.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas.

2.1.3.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

2.1.3.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.1.3.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.1.3.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas.

2.1.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

2.1.3.2.12. Capacidade de verificar objetos usando heurística.

2.1.3.2.13. Capacidade de agendar uma pausa na verificação.

2.1.3.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias.

2.1.3.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

2.1.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.1.3.2.16.1. Perguntar o que fazer, ou;

2.1.3.2.16.2. Bloquear acesso ao objeto.

2.1.3.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.3.2.16.2.2. Caso positivo de desinfecção:

2.1.3.2.16.2.2.1. Restaurar o objeto para uso.

2.1.3.2.16.2.3. Caso negativo de desinfecção:

2.1.3.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.1.3.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI.

2.1.3.2.19. Capacidade de verificar links inseridos em e-mails contra phishings.

2.1.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

2.1.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

2.1.3.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

2.1.3.2.22.1. Perguntar o que fazer, ou;

2.1.3.2.22.2. Bloquear o e-mail.

2.1.3.2.22.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.3.2.22.2.2. Caso positivo de desinfecção:

2.1.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

2.1.3.2.22.2.3. Caso negativo de desinfecção:

2.1.3.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.3.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

2.1.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

2.1.3.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.

2.1.3.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script etc.), usando heurísticas.

2.1.3.2.27. Deve ter suporte total ao protocolo Ipv6.

2.1.3.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail.

2.1.3.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

2.1.3.2.29.1. Perguntar o que fazer, ou;

2.1.3.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.1.3.2.29.3. Permitir acesso ao objeto.

2.1.3.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

2.1.3.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

2.1.3.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

2.1.3.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

2.1.3.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.

2.1.3.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

2.1.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

2.1.3.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

2.1.3.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica.

2.1.3.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

2.1.3.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.1.3.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas.

2.1.3.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.1.3.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

2.1.3.2.39.1. Discos de armazenamento locais.

2.1.3.2.39.2. Armazenamento removível.

2.1.3.2.39.3. Impressoras.

2.1.3.2.39.4. CD/DVD.

2.1.3.2.39.5. Drives de disquete.

2.1.3.2.39.6. Modems.

2.1.3.2.39.7. Dispositivos de fita.

2.1.3.2.39.8. Dispositivos multifuncionais.

2.1.3.2.39.9. Leitores de smart card.

2.1.3.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile etc.).

2.1.3.2.39.11. Wi-Fi.

2.1.3.2.39.12. Adaptadores de rede externos.

2.1.3.2.39.13. Dispositivos MP3 ou smartphones.

2.1.3.2.39.14. Dispositivos Bluetooth.

2.1.3.2.39.15. Câmeras e Scanners.

2.1.3.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário.

2.1.3.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

2.1.3.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

2.1.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

2.1.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

2.1.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

2.1.3.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

2.1.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.1.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.1.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

2.1.3.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.

2.1.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.1.3.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.1.3.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

2.1.3.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

2.1.3.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.1.3.2.54. Capacidade de integração com o Windows Defender Security Center.

2.1.3.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).

2.1.3.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

2.1.4. Estações Mac OS X

2.1.4.1. Compatibilidade:

2.1.4.1.1. OS X 10.9 (Mavericks).

2.1.4.1.2. OS X 10.10 (Yosemite).

2.1.4.1.3. OS X 10.11 (El Capitan).

2.1.4.1.4. macOS 10.12 (Sierra).

2.1.4.1.5. macOS 10.13 (High Sierra).

2.1.4.1.6. macOS 10.14 (Mojave).

2.1.4.1.7. macOS 10.15 (Catalina).

2.1.4.1.8. macOS 11.0 (Big Sur).

2.1.4.2. Características:

2.1.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.1.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https.

2.1.4.2.3. Possuir módulo de bloqueio a ataques na rede.

2.1.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador.

2.1.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

2.1.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

2.1.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

2.1.4.2.8. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.1.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

2.1.4.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

2.1.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

2.1.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

2.1.4.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.1.4.2.14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

2.1.4.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.1.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

2.1.4.2.17. Capacidade de verificar objetos usando heurística.

2.1.4.2.18. Capacidade de agendar uma pausa na verificação.

2.1.4.2.19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.1.4.2.19.1. Perguntar o que fazer, ou;

2.1.4.2.19.2. Bloquear acesso ao objeto.

2.1.4.2.19.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.4.2.19.3.1. Caso positivo de desinfecção:

2.1.4.2.19.3.1.1. Restaurar o objeto para uso.

2.1.4.2.19.3.2. Caso negativo de desinfecção:

2.1.4.2.19.3.2.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.4.2.20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.1.4.2.21. Capacidade de verificar arquivos de formato de email.

2.1.4.2.22. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, parar o antivírus e iniciar o antivírus pela linha de comando.

2.1.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

2.1.5. Estações Linux

2.1.5.1. Compatibilidade:

2.1.5.1.1. Plataforma 32 bits:

2.1.5.1.1.1. Ubuntu 16.04 LTS

2.1.5.1.1.2. Red Hat® Enterprise Linux® 6.7

2.1.5.1.1.3. CentOS-6.7

2.1.5.1.1.4. Debian GNU / Linux 9.4

2.1.5.1.2. Plataforma 64 bits:

2.1.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

2.1.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

2.1.5.1.2.3. CentOS-6.7, 7.2, 8.0

2.1.5.1.2.4. Debian GNU / Linux 9.4, 10.1

2.1.5.1.2.5. OracleLinux 7.3, 8

2.1.5.1.2.6. SUSE® Linux Enterprise Server 15

2.1.5.1.2.7. openSUSE® 15

2.1.5.1.2.8. Amazon Linux AMI

2.1.5.2. Características

2.1.5.2.1. Deve prover as seguintes proteções:

2.1.5.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.1.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

2.1.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

2.1.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

2.1.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

2.1.5.2.7. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.1.5.2.8. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.1.5.2.9. Capacidade de criar exclusões por local, máscara e nome da ameaça.

2.1.5.2.10. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.1.5.2.11. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

2.1.5.2.12. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers.

2.1.5.2.13. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

2.1.5.2.13.1. Alta.

2.1.5.2.13.2. Média.

2.1.5.2.13.3. Baixa.

2.1.5.2.13.4. Recomendado.

2.1.5.2.14. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

2.1.5.2.15. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos. desinfecção ou remoção de objetos infectados.

2.1.5.2.16. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

2.1.5.2.17. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.1.5.2.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.1.5.2.19. Capacidade de verificar objetos usando heurística.

2.1.5.2.20. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.1.5.2.21. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

2.1.6. Servidores Windows

2.1.6.1. Compatibilidade:

2.1.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

2.1.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

2.1.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

2.1.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

2.1.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

2.1.6.1.6. Microsoft Windows Server 2016.

2.1.6.1.7. Microsoft Windows Server 2019.

2.1.6.2. Características:

2.1.6.2.1. Deve prover as seguintes proteções:

2.1.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.1.6.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus.

2.1.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

2.1.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

2.1.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.1.6.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.1.6.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.1.6.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.1.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

2.1.6.2.4.3. Leitura de configurações.

2.1.6.2.4.4. Modificação de configurações.

2.1.6.2.4.5. Gerenciamento de Backup e Quarentena.

2.1.6.2.4.6. Visualização de relatórios.

2.1.6.2.4.7. Gerenciamento de relatórios.

2.1.6.2.4.8. Gerenciamento de chaves de licença.

2.1.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

2.1.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

2.1.6.2.6. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede.

2.1.6.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros etc.).

2.1.6.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS).

2.1.6.2.9. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares.

2.1.6.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

2.1.6.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.

2.1.6.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

2.1.6.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

2.1.6.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.1.6.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.1.6.2.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.1.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

2.1.6.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (exemplo: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários etc.).

2.1.6.2.19. Capacidade de verificar objetos usando heurística.

2.1.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

2.1.6.2.21. Capacidade de agendar uma pausa na verificação.

2.1.6.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

2.1.6.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.1.6.2.23.1. Perguntar o que fazer, ou;

2.1.6.2.23.2. Bloquear acesso ao objeto.

2.1.6.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.6.2.23.2.2. Caso positivo de desinfecção:

2.1.6.2.23.2.2.1. Restaurar o objeto para uso.

2.1.6.2.23.3. Caso negativo de desinfecção:

2.1.6.2.23.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.1.6.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.1.6.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.1.6.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

2.1.6.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

2.1.6.2.28. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

2.1.6.2.29. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.1.6.2.30. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

2.1.7. Servidores Linux

2.1.7.1. Compatibilidade:

2.1.7.1.1. Plataforma 32 bits:

2.1.7.1.1.1. Ubuntu 16.04 LTS.

2.1.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

2.1.7.1.1.3. CentOS-6.7.

2.1.7.1.1.4. Debian GNU / Linux 9.4.

2.1.7.1.2. Plataforma 64 bits:

2.1.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

2.1.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

2.1.7.1.2.3. CentOS-6.7, 7.2, 8.0.

2.1.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

2.1.7.1.2.5. OracleLinux 7.3, 8.

2.1.7.1.2.6. SUSE® Linux Enterprise Server 15.

2.1.7.1.2.7. openSUSE® 15.

2.1.7.1.2.8. Amazon Linux AMI.

2.1.7.2. Características:

2.1.7.2.1. Deve prover as seguintes proteções:

2.1.7.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.1.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

2.1.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

2.1.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

2.1.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

2.1.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

2.1.7.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.1.7.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.1.7.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.1.7.2.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

2.1.7.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

2.1.7.2.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

2.1.7.2.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

2.1.7.2.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.1.7.2.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.1.7.2.7. Capacidade de verificar objetos usando heurística.

2.1.7.2.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.1.7.2.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

2.1.7.2.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

2.1.8. Smartphones e tablets

2.1.8.1. Compatibilidade:

2.1.8.1.1. Dispositivos com os sistemas operacionais:

2.1.8.1.1.1. Android 4.2 – 11.

2.1.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

2.1.8.2. Características:

2.1.8.2.1. Deve prover as seguintes proteções:

2.1.8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

2.1.8.2.1.2. Proteção contra adware e autodialers.

2.1.8.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.

2.1.8.2.1.4. Arquivos abertos no smartphone.

2.1.8.2.1.5. Programas instalados usando a interface do smartphone

2.1.8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento.

2.1.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

2.1.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

2.1.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

2.1.8.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.

2.1.8.2.6. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha.

2.1.8.2.7. Deverá ter firewall pessoal (Android).

2.1.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

2.1.8.2.9. Capacidade de enviar comandos remotamente de:

2.1.8.2.9.1. Localizar.

2.1.8.2.9.2. Bloquear.

2.1.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

2.1.8.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos.

2.1.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

2.1.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

2.1.8.2.14. Capacidade de localizar o dispositivo quando necessário.

2.1.8.2.15. Permitir atualização das definições quando estiver em "roaming".

2.1.8.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus.

2.1.8.2.17. Deve permitir verificar somente arquivos executáveis.

2.1.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

2.1.8.2.19. Capacidade de agendar uma verificação.

2.1.8.2.20. Capacidade de enviar URL de instalação por e-mail.

2.1.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

2.1.8.2.22. Capacidade de executar as seguintes ações caso a desinfecção falhe:

2.1.8.2.22.1. Deletar.

2.1.8.2.22.2. Ignorar.

2.1.8.2.22.3. Quarentenar.

2.1.8.2.22.4. Perguntar ao usuário.

2.1.9. Gerenciamento de dispositivos móveis (MDM):

2.1.9.1. Compatibilidade:

2.1.9.1.1. Android 4.2 – 11.

2.1.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

2.1.9.2. Características:

2.1.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

2.1.9.2.2. Capacidade de ajustar as configurações de:

2.1.9.2.2.1. Sincronização de e-mail.

2.1.9.2.2..2. Uso de aplicativos.

2.1.9.2.2.3. Senha do usuário.

2.1.9.2.2.4. Criptografia de dados.

2.1.9.2.2.5. Conexão de mídia removível.

2.1.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

2.1.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

2.1.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

2.1.9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS.

2.1.9.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento.

2.1.9.2.8. Permitir sincronização com perfil do "Touch Down".

2.1.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

2.1.9.2.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual.

2.1.9.2.11. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

2.2. Aquisição de licenças de solução corporativa de antivírus

2.2.1. Características Gerais

2.2.1.1. Todas as licenças fornecidas terão validade de 36 (trinta e seis) meses para atualizações inerentes ao produto.

2.2.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

2.2.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

2.2.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para o Contratante além daquele já cotado na proposta.

2.2.2. Servidor de Administração e Console Administrativa

2.2.2.1. Compatibilidade:

2.2.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

2.2.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

2.2.2.1.3. Microsoft Windows Server 2016 x64.

2.2.2.1.4. Microsoft Windows Server 2019 x64.

2.2.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

2.2.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

2.2.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

2.2.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

2.2.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

2.2.2.2. Características:

2.2.2.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC.

2.2.2.2.2. Console deve ser baseada no modelo cliente/servidor.

2.2.2.2.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.

2.2.2.2.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.

2.2.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

2.2.2.2.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM.

2.2.2.2.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores.

2.2.2.2.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory.

2.2.2.2.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.

2.2.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

2.2.2.2.11. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada.

2.2.2.2.12. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas.

2.2.2.2.13. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas.

2.2.2.2.14. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador.

2.2.2.2.15. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle.

2.2.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

2.2.2.2.17. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus.

2.2.2.2.18. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança.

2.2.2.2.19. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede.

2.2.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

2.2.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

2.2.2.2.22. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes.

2.2.2.2.23. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

2.2.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

2.2.2.2.25. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

2.2.2.2.25.1. Nome do computador.

2.2.2.2.25.2. Nome do domínio.

2.2.2.2.25.3. Range de IP.

2.2.2.2.25.4. Sistema Operacional.

2.2.2.2.25.5. Máquina virtual.

2.2.2.2.26. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas.

2.2.2.2.27. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional.

2.2.2.2.28. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção.

2.2.2.2.29. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção.

2.2.2.2.30. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente.

2.2.2.2.31. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias etc.

2.2.2.2.32. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos.

2.2.2.2.33. Deve fornecer as seguintes informações dos computadores:

2.2.2.2.33.1. Se o antivírus está instalado.

2.2.2.2.33.2. Se o antivírus está iniciado.

2.2.2.2.33.3. Se o antivírus está atualizado.

2.2.2.2.33.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo.

2.2.2.2.33.5. Minutos/horas desde a última atualização de vacinas.

2.2.2.2.33.6. Data e horário da última verificação executada na máquina.

2.2.2.2.33.7. Versão do antivírus instalado na máquina.

2.2.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças.

2.2.2.2.33.9. Data e horário de quando a máquina foi ligada.

2.2.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina.

2.2.2.2.33.11. Nome do computador.

2.2.2.2.33.12. Domínio ou grupo de trabalho do computador.

2.2.2.2.33.13. Data e horário da última atualização de vacinas.

2.2.2.2.33.14. Sistema operacional com Service Pack.

2.2.2.2.33.15. Quantidade de processadores.

2.2.2.2.33.16. Quantidade de memória RAM.

2.2.2.2.33.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory).

2.2.2.2.33.18. Endereço IP.

2.2.2.2.33.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.

2.2.2.2.33.20. Atualizações do Windows Updates instaladas.

2.2.2.2.33.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD.

2.2.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina.

2.2.2.2.34. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las.

2.2.2.2.35. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

2.2.2.2.35.1. Alteração de Gateway Padrão.

2.2.2.2.35.2. Alteração de subrede.

2.2.2.2.35.3. Alteração de domínio.

2.2.2.2.35.4. Alteração de servidor DHCP.

2.2.2.2.35.5. Alteração de servidor DNS.

2.2.2.2.35.6. Alteração de servidor WINS.

2.2.2.2.35.7. Alteração de subrede.

2.2.2.2.35.8. Resolução de Nome.

2.2.2.2.35.9. Disponibilidade de endereço de conexão SSL.

2.2.2.2.36. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet.

2.2.2.2.37. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes.

2.2.2.2.38. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus.

2.2.2.2.39. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos.

2.2.2.2.40. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede.

2.2.2.2.41. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.

2.2.2.2.42. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

2.2.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos.

2.2.2.2.44. Capacidade de enviar e-mails para contas específicas em caso de algum evento.

2.2.2.2.45. Listar em um único local, todos os computadores não gerenciados na rede.

2.2.2.2.46. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes.

2.2.2.2.47. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

2.2.2.2.48. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação etc.), inclusive de máquinas que estejam em subnets diferentes do servidor.

2.2.2.2.49. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo).

2.2.2.2.50. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador.

2.2.2.2.51. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (exemplo: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint).

2.2.2.2.52. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação.

2.2.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

2.2.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

2.2.2.2.55. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

2.2.2.2.55.1. Nome do vírus.

2.2.2.2.55.2. Nome do arquivo infectado.

2.2.2.2.55.3. Data e hora da detecção.

2.2.2.2.55.4. Nome da máquina ou endereço IP.

2.2.2.2.55.5. Ação realizada.

2.2.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

2.2.2.2.57. Capacidade de listar updates nas máquinas com o respectivo link para download.

2.2.2.2.58. Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração.

2.2.2.2.59. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante.

2.2.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente.

2.2.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2.2.3. Estações Windows

2.2.3.1. Compatibilidade:

2.2.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate.

2.2.3.1.2. Microsoft Windows 8 Professional/Enterprise.

2.2.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

2.2.3.1.4. Microsoft Windows 10 Professional/Enterprise.

2.2.3.2. Características:

2.2.3.2.1. Deve prover as seguintes proteções:

2.2.3.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.3.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus).

2.2.3.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos).

2.2.3.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza.

2.2.3.2.1.5. Firewall com IDS.

2.2.3.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus).

2.2.3.2.1.7. Controle de dispositivos externos.

2.2.3.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

2.2.3.2.1.9. Controle de acesso a sites por horário.

2.2.3.2.1.10. Controle de acesso a sites por usuários.

2.2.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

2.2.3.2.1.12. Controle de execução de aplicativos.

2.2.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

2.2.3.2.2.Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.2.3.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

2.2.3.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

2.2.3.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (exemplo: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.2.3.2.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas.

2.2.3.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

2.2.3.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.2.3.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.2.3.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas.

2.2.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

2.2.3.2.12. Capacidade de verificar objetos usando heurística.

2.2.3.2.13. Capacidade de agendar uma pausa na verificação.

2.2.3.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias.

2.2.3.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

2.2.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.2.3.2.16.1. Perguntar o que fazer, ou;

2.2.3.2.16.2. Bloquear acesso ao objeto.

2.2.3.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.3.2.16.2.2. Caso positivo de desinfecção:

2.2.3.2.16.2.2.1. Restaurar o objeto para uso.

2.2.3.2.16.2.3. Caso negativo de desinfecção:

2.2.3.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.2.3.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI.

2.2.3.2.19. Capacidade de verificar links inseridos em e-mails contra phishings.

2.2.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

2.2.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

2.2.3.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

2.2.3.2.22.1. Perguntar o que fazer, ou;

2.2.3.2.22.2. Bloquear o e-mail.

2.2.3.2.22.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.3.2.22.2.2. Caso positivo de desinfecção:

2.2.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

2.2.3.2.22.2.3. Caso negativo de desinfecção:

2.2.3.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.3.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

2.2.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

2.2.3.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.

2.2.3.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script etc.), usando heurísticas.

2.2.3.2.27. Deve ter suporte total ao protocolo Ipv6.

2.2.3.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail.

2.2.3.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

2.2.3.2.29.1. Perguntar o que fazer, ou;

2.2.3.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.2.3.2.29.3. Permitir acesso ao objeto.

2.2.3.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

2.2.3.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

2.2.3.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

2.2.3.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

2.2.3.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.

2.2.3.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

2.2.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

2.2.3.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

2.2.3.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica.

2.2.3.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

2.2.3.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.2.3.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas.

2.2.3.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.2.3.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

2.2.3.2.39.1. Discos de armazenamento locais.

2.2.3.2.39.2. Armazenamento removível.

2.2.3.2.39.3. Impressoras.

2.2.3.2.39.4. CD/DVD.

2.2.3.2.39.5. Drives de disquete.

2.2.3.2.39.6. Modems.

2.2.3.2.39.7. Dispositivos de fita.

2.2.3.2.39.8. Dispositivos multifuncionais.

2.2.3.2.39.9. Leitores de smart card.

2.2.3.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile etc.).

2.2.3.2.39.11. Wi-Fi.

2.2.3.2.39.12. Adaptadores de rede externos.

2.2.3.2.39.13. Dispositivos MP3 ou smartphones.

2.2.3.2.39.14. Dispositivos Bluetooth.

2.2.3.2.39.15. Câmeras e Scanners.

2.2.3.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário.

2.2.3.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

2.2.3.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

2.2.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

2.2.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

2.2.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

2.2.3.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

2.2.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.2.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.2.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

2.2.3.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.

2.2.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.2.3.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.2.3.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

2.2.3.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

2.2.3.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.2.3.2.54. Capacidade de integração com o Windows Defender Security Center.

2.2.3.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).

2.2.3.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

2.2.4. Estações Mac OS X

2.2.4.1. Compatibilidade:

2.2.4.1.1. OS X 10.9 (Mavericks).

2.2.4.1.2. OS X 10.10 (Yosemite).

2.2.4.1.3. OS X 10.11 (El Capitan).

2.2.4.1.4. macOS 10.12 (Sierra).

2.2.4.1.5. macOS 10.13 (High Sierra).

2.2.4.1.6. macOS 10.14 (Mojave).

2.2.4.1.7. macOS 10.15 (Catalina).

2.2.4.1.8. macOS 11.0 (Big Sur).

2.2.4.2. Características:

2.2.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https.

2.2.4.2.3. Possuir módulo de bloqueio a ataques na rede.

2.2.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador.

2.2.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

2.2.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

2.2.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

2.2.4.2.8. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.2.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

2.2.4.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

2.2.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

2.2.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

2.2.4.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.2.4.2.14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

2.2.4.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.2.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

2.2.4.2.17. Capacidade de verificar objetos usando heurística.

2.2.4.2.18. Capacidade de agendar uma pausa na verificação.

2.2.4.2.19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.2.4.2.19.1. Perguntar o que fazer, ou;

2.2.4.2.19.2. Bloquear acesso ao objeto.

2.2.4.2.19.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.4.2.19.3.1. Caso positivo de desinfecção:

2.2.4.2.19.3.1.1. Restaurar o objeto para uso.

2.2.4.2.19.3.2. Caso negativo de desinfecção:

2.2.4.2.19.3.2.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.4.2.20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.2.4.2.21. Capacidade de verificar arquivos de formato de email.

2.2.4.2.22. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, parar o antivírus e iniciar o antivírus pela linha de comando.

2.2.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

2.2.5. Estações Linux

2.2.5.1. Compatibilidade:

2.2.5.1.1. Plataforma 32 bits:

2.2.5.1.1.1. Ubuntu 16.04 LTS

2.2.5.1.1.2. Red Hat® Enterprise Linux® 6.7

2.2.5.1.1.3. CentOS-6.7

2.2.5.1.1.4. Debian GNU / Linux 9.4

2.2.5.1.2. Plataforma 64 bits:

2.2.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

2.2.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

2.2.5.1.2.3. CentOS-6.7, 7.2, 8.0

2.2.5.1.2.4. Debian GNU / Linux 9.4, 10.1

2.2.5.1.2.5. OracleLinux 7.3, 8

2.2.5.1.2.6. SUSE® Linux Enterprise Server 15

2.2.5.1.2.7. openSUSE® 15

2.2.5.1.2.8. Amazon Linux AMI

2.2.5.2. Características

2.2.5.2.1. Deve prover as seguintes proteções:

2.2.5.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

2.2.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

2.2.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

2.2.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

2.2.5.2.7. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.2.5.2.8. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.2.5.2.9. Capacidade de criar exclusões por local, máscara e nome da ameaça.

2.2.5.2.10. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.2.5.2.11. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

2.2.5.2.12. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers.

2.2.5.2.13. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

2.2.5.2.13.1. Alta.

2.2.5.2.13.2. Média.

2.2.5.2.13.3. Baixa.

2.2.5.2.13.4. Recomendado.

2.2.5.2.14. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

2.2.5.2.15. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos. desinfecção ou remoção de objetos infectados.

2.2.5.2.16. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

2.2.5.2.17. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.2.5.2.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.2.5.2.19. Capacidade de verificar objetos usando heurística.

2.2.5.2.20. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.2.5.2.21. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

2.2.6. Servidores Windows

2.2.6.1. Compatibilidade:

2.2.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

2.2.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

2.2.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

2.2.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

2.2.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

2.2.6.1.6. Microsoft Windows Server 2016.

2.2.6.1.7. Microsoft Windows Server 2019.

2.2.6.2. Características:

2.2.6.2.1. Deve prover as seguintes proteções:

2.2.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.6.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus.

2.2.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

2.2.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

2.2.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.2.6.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.2.6.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.2.6.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.2.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

2.2.6.2.4.3. Leitura de configurações.

2.2.6.2.4.4. Modificação de configurações.

2.2.6.2.4.5. Gerenciamento de Backup e Quarentena.

2.2.6.2.4.6. Visualização de relatórios.

2.2.6.2.4.7. Gerenciamento de relatórios.

2.2.6.2.4.8. Gerenciamento de chaves de licença.

2.2.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

2.2.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

2.2.6.2.6. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede.

2.2.6.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros etc.).

2.2.6.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS).

2.2.6.2.9. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares.

2.2.6.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

2.2.6.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.

2.2.6.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

2.2.6.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

2.2.6.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

2.2.6.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.2.6.2.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.2.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

2.2.6.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (exemplo: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários etc.).

2.2.6.2.19. Capacidade de verificar objetos usando heurística.

2.2.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

2.2.6.2.21. Capacidade de agendar uma pausa na verificação.

2.2.6.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

2.2.6.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.2.6.2.23.1. Perguntar o que fazer, ou;

2.2.6.2.23.2. Bloquear acesso ao objeto.

2.2.6.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.6.2.23.2.2. Caso positivo de desinfecção:

2.2.6.2.23.2.2.1. Restaurar o objeto para uso.

2.2.6.2.23.3. Caso negativo de desinfecção:

2.2.6.2.23.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

2.2.6.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.2.6.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.2.6.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

2.2.6.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

2.2.6.2.28. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

2.2.6.2.29. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.2.6.2.30. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

2.2.7. Servidores Linux

2.2.7.1. Compatibilidade:

2.2.7.1.1. Plataforma 32 bits:

2.2.7.1.1.1. Ubuntu 16.04 LTS.

2.2.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

2.2.7.1.1.3. CentOS-6.7.

2.2.7.1.1.4. Debian GNU / Linux 9.4.

2.2.7.1.2. Plataforma 64 bits:

2.2.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

2.2.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

2.2.7.1.2.3. CentOS-6.7, 7.2, 8.0.

2.2.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

2.2.7.1.2.5. OracleLinux 7.3, 8.

2.2.7.1.2.6. SUSE® Linux Enterprise Server 15.

2.2.7.1.2.7. openSUSE® 15.

2.2.7.1.2.8. Amazon Linux AMI.

2.2.7.2. Características:

2.2.7.2.1. Deve prover as seguintes proteções:

2.2.7.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

2.2.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

2.2.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

2.2.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

2.2.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

2.2.7.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.2.7.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.2.7.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

2.2.7.2.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

2.2.7.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

2.2.7.2.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

2.2.7.2.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

2.2.7.2.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

2.2.7.2.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

2.2.7.2.7. Capacidade de verificar objetos usando heurística.

2.2.7.2.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

2.2.7.2.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

2.2.7.2.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

2.2.8. Smartphones e tablets

2.2.8.1. Compatibilidade:

2.2.8.1.1. Dispositivos com os sistemas operacionais:

2.2.8.1.1.1. Android 4.2 – 11.

2.2.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

2.2.8.2. Características:

2.2.8.2.1. Deve prover as seguintes proteções:

2.2.8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

2.2.8.2.1.2. Proteção contra adware e autodialers.

2.2.8.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.

2.2.8.2.1.4. Arquivos abertos no smartphone.

2.2.8.2.1.5. Programas instalados usando a interface do smartphone

2.2.8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento.

2.2.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

2.2.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

2.2.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

2.2.8.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.

2.2.8.2.6. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha.

2.2.8.2.7. Deverá ter firewall pessoal (Android).

2.2.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

2.2.8.2.9. Capacidade de enviar comandos remotamente de:

2.2.8.2.9.1. Localizar.

2.2.8.2.9.2. Bloquear.

2.2.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

2.2.8.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos.

2.2.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

2.2.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

2.2.8.2.14. Capacidade de localizar o dispositivo quando necessário.

2.2.8.2.15. Permitir atualização das definições quando estiver em "roaming".

2.2.8.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus.

2.2.8.2.17. Deve permitir verificar somente arquivos executáveis.

2.2.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

2.2.8.2.19. Capacidade de agendar uma verificação.

2.2.8.2.20. Capacidade de enviar URL de instalação por e-mail.

2.2.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

2.2.8.2.22. Capacidade de executar as seguintes ações caso a desinfecção falhe:

2.2.8.2.22.1. Deletar.

2.2.8.2.22.2. Ignorar.

2.2.8.2.22.3. Quarentenar.

2.2.8.2.22.4. Perguntar ao usuário.

2.2.9. Gerenciamento de dispositivos móveis (MDM):

2.2.9.1. Compatibilidade:

2.2.9.1.1. Android 4.2 – 11.

2.2.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

2.2.9.2. Características:

2.2.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

2.2.9.2.2. Capacidade de ajustar as configurações de:

2.2.9.2.2.1. Sincronização de e-mail.

2.2.9.2.2..2. Uso de aplicativos.

2.2.9.2.2.3. Senha do usuário.

2.2.9.2.2.4. Criptografia de dados.

2.2.9.2.2.5. Conexão de mídia removível.

2.2.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

2.2.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

2.2.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

2.2.9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS.

2.2.9.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento.

2.2.9.2.8. Permitir sincronização com perfil do "Touch Down".

2.2.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

2.2.9.2.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual.

2.2.9.2.11. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

2.3. Transferência de conhecimento e direitos de propriedade intelectual

2.3.1. O uso de uma solução de antivírus corporativo é imprescindível por conter funções de proteção que vão além de um antivírus comum, evitando, portanto, invasões ou roubos de informações, por exemplo. Por isso, não existe versões

corporativas gratuitas, não sendo vislumbrada outra forma de utilização senão a obrigatoriedade da renovação/aquisição dessa tecnologia de terceiros.

2.3.2. Os antivírus corporativos são produtos consolidados no mercado de Tecnologia da Informação e Comunicação no Brasil e utilizados por organizações públicas e privadas. Desta forma, os riscos de descontinuidade desse produto no mercado parecem ser mínimos.

2.3.3. A Contratada deverá realizar a transferência de conhecimento nas versões dos softwares que serão adquiridos pelo Contratante e com isso, repassar informações de configuração, testes, procedimentos de contingência e demais informações necessárias para a operação e manutenção da solução.

2.3.4. Não se aplica o requisito pertinente aos direitos de propriedade intelectual e autoral da STIC, uma vez que não será produzido nenhum artefato, tampouco trata de desenvolvimento de software.

3. GARANTIA E SUPORTE

3.1. Garantia

3.1.1. Durante o período de vigência do contrato a garantia se dará em forma de suporte técnico e seguirá as especificações descritas no Termo de Referência que tratarão as respostas a incidentes de segurança.

3.1.2. A Contratada deverá prestar garantia, com o fornecimento de novas versões, pelo período de 36 (trinta e seis) meses, contados a partir da assinatura do Termo de Recebimento Definitivo.

3.1.3. Incluem-se, na garantia, os serviços de manutenção, suporte técnico, atualização de software e produto, bem como o auxílio na utilização de recursos ou solução de problemas relacionados aos softwares ofertados.

3.2. Suporte Técnico

3.2.1. Durante a vigência do contrato deverá ser fornecido suporte técnico pela Contratada seguindo as especificações abaixo:

3.2.1.1. Apoio às respostas a incidentes de segurança envolvendo malware.

3.2.1.2. Suporte técnico para eventuais dúvidas ou problemas com a solução.

3.2.1.3. Acompanhamento nos chamados escalados para o Fabricante em situações de falhas/problemas desconhecidos pelo suporte técnico da Contratada ou bugs.

3.2.1.4. O atendimento deverá ser realizado via contato telefônico ou ferramenta de acesso remoto independentemente do tipo de incidente.

3.2.1.5. Suporte técnico 8x5, prestado unicamente à equipe de segurança da área de tecnologia do Contratante, referente a problemas de funcionamento/configuração dos produtos fornecidos.

3.2.1.6. Número de chamados ilimitados;

3.2.2. Incidentes, chamados, e problemas escalados ao Fabricante deverão atender os prazos estabelecidos na tabela abaixo:

Níveis de Severidade	Descrição	Prazo para solução
Nível 1 – Crítico	Afeta o serviço prestado pelo Contratante por interrupções da solução de antivírus nos sistemas operacionais, possíveis perda de dados, alterações de configuração padrão para configuração insegura e onde não há solução alternativa disponível.	6 horas
Nível 2 – Alto	Afeta a funcionalidade do produto, mas não causa corrupção e perda de dados ou travamento sistemas.	10 horas
Nível 3 – Médio	Solicitações não críticas, as quais não afetam a funcionalidade do produto.	12 horas
Nível 4 – Baixo	Solicitações não críticas ou solicitação de serviços. Todos os incidentes que não satisfaçam um dos critérios listados acima, serão classificados a esse nível de gravidade.	14 horas

3.2.3. Será respeitado o horário de expediente do Contratante, caso o prazo de solução expire em horário não comercial, a contagem do prazo de solução será paralisada no final do expediente e iniciada no próximo dia útil, contando o prazo de solução já decorrido do chamando no dia anterior.

3.2.4. A Contratada deverá prestar suporte técnico e operacional durante o período de vigência da licença, com atendimento através do serviço telefônico (0800), acesso remoto, e-mail ou WEB, para esclarecimento de dúvidas, abertura de chamados, e envio de arquivos para análise.

3.2.5. Ambos os objetos 1) Renovação de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select; e 2) Aquisição de licenças do software de antivírus Kaspersky Endpoint Security – Versão Business Select deverão ser atendidos com essas exigências de suporte técnico.

4. GESTÃO E FISCALIZAÇÃO CONTRATUAL

4.1. Profissionais da Contratada: equipe composta por técnicos da Contratada, responsáveis pela execução e acompanhamento do objeto.

4.1.1. Técnico: funcionário da Contratada, responsável pela execução técnica-operacional.

4.1.2. Preposto: funcionário representante da Contratada, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

4.2. Equipe de Gestão do Contrato: equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares.

4.2.1. Gestor do Contrato: servidor responsável pela gestão contratual, conforme Decreto Judiciário nº 291, de 2009 e Portaria nº 255, de 2009, do Tribunal de Justiça do Estado do Tocantins.

4.2.2. Fiscal Demandante: servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos funcionais da solução.

4.2.3. Fiscal Técnico: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.

4.2.4. Fiscal Administrativo: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

4.3. A atuação ou a eventual omissão da Fiscalização durante a realização dos trabalhos, não poderá ser invocada para eximir a Contratada da responsabilidade no fornecimento dos produtos.

4.4. A fiscalização será sob o aspecto qualitativo e quantitativo, devendo ser anotado, em registro próprio as falhas detectadas, e comunicadas ao gestor do contrato todas as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte da Contratada.

4.5. A comunicação entre a fiscalização e a Contratada será realizada por meio de correspondência oficial e anotações ou registros no mesmo processo que tratam da aquisição dos objetos.

4.6. Quando houver necessidade o gestor deverá emitir notificações para a Contratada.

5. DINÂMICA DE EXECUÇÃO

5.1. A tabela abaixo sintetiza as etapas de execução desta contratação. O prazo em todas as etapas tem como referência inicial o fim da etapa anterior.

Etapa	Descrição	Quando ocorre
1	Recebimento do pedido de fornecimento.	O TJTO encaminhará o pedido de fornecimento a qualquer tempo dentro da vigência da Ata de Registro de Preços e após a assinatura do contrato.
2	Entrega das licenças.	O prazo será de até 20 (vinte) dias úteis, contados a partir da data de assinatura do contrato ou recebimento da nota de empenho.
3	Recebimento	Imediatamente após o recebimento das licenças, para

	provisório das licenças.	efeito de posterior verificação da conformidade do material com a especificação, nos termos do artigo 73, da Lei nº 8.666, de 1993.
4	Avaliação das licenças entregues.	Após a entrega, será realizada uma avaliação e homologação pelos responsáveis técnicos. A análise para comprovação das características técnicas consistirá em avaliar as documentações apresentadas e também informações de registro das licenças no site oficial do fabricante.
5	Recebimento Definitivo das licenças.	O responsável técnico deverá, após a comprovação do atendimento das especificações técnicas, emitir e assinar em, no máximo, 15 (quinze) dias úteis, contados do primeiro dia útil posterior à entrega dos equipamentos, o Termo de Recebimento Definitivo, nos termos do artigo 73, da Lei nº 8.666, de 1993.
6	Início da contagem do prazo de garantia.	Data da emissão do recebimento definitivo das licenças. Se for o caso de licenças vincendas, a garantia iniciará no dia subsequente após o fim da vigência desta.
7	Fim do prazo de garantia	Após 36 (trinta e seis) meses.

6. DO RECEBIMENTO

6.1. O Tribunal de Justiça expedirá "Termo de Recebimento Provisório", o qual deverá ser assinado pelo gestor, para efeito de posterior verificação da conformidade dos objetos com as especificações constantes neste Termo de Referência, nos termos do artigo 73, da Lei nº 8.666, de 1993.

6.2. Após a verificação da qualidade e quantidade do material e consequente aceitação, nos termos do artigo 73, da Lei nº 8.666, de 1993, o Tribunal de Justiça emitirá "Termo de Recebimento Definitivo", no prazo de 15 (quinze) dias, o qual deverá ser assinado pelo gestor.

6.3. O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com este termo de referência.

6.4. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato.

6.5. O Fornecedor é obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

7. DO PAGAMENTO

7.1. O Fornecedor deverá apresentar nota fiscal, correspondente aos produtos efetivamente entregues.

7.2. O Contratante reserva-se o direito de não realizar o atesto, se os dados estiverem em desacordo com os dados do Fornecedor ou, ainda, se o objeto entregue não estiver em conformidade com as especificações apresentadas neste Termo de Referência, ficando o pagamento suspenso até a regularização.

7.3. O atesto do gestor é condição indispensável para o pagamento.

7.4. Na ausência do fiscal do contrato (férias, licença ou em viagem por interesse do Poder Judiciário), o atesto será dado pelo gestor substituto.

7.5. O pagamento será efetuado em até 30 (trinta) dias corridos, contados a partir do protocolo de recebimento da nota fiscal, sendo que, recaindo sobre dias não úteis, o termo final será prorrogado para o dia útil subsequente.

7.6. O CNPJ deverá ser o mesmo indicado na proposta, nota de empenho e vinculado à conta corrente do Fornecedor.

7.7. Todos os atos inerentes ao presente processo obedecerão às regras concernentes ao Sistema de Eletrônico de Informação do Tribunal de Justiça do Estado do Tocantins – SEI.

8. DA ATA DE REGISTRO DE PREÇOS

8.1. A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da sua publicação.

9. DO CONTRATO

9.1. Caso exista demanda dos objetos registrados e havendo orçamento para realizar a contratação, o Tribunal de Justiça do Estado do Tocantins firmará contrato para adquiri-los nos quantitativos necessários para suprir suas necessidades.

9.2. No ato de assinatura do contrato, a Contratada deverá atender as disposições da Portaria nº 97, de 2010, quanto à verificação da regularidade fiscal. Se qualquer das certidões apresentadas na fase de habilitação do procedimento licitatório expirar sua validade antes da data de assinatura dos contratos ou de seus aditivos, deverá ser atualizada.

9.3. Os contratos a serem firmados terão vigência de 36 (trinta e seis) meses, contados a partir do recebimento definitivo da solução adquirida.

10. SANÇÕES ADMINISTRATIVAS

10.1. A empresa que, convocada dentro do prazo de validade da sua proposta, não celebrar o contrato, quando exigido, deixar de entregar a documentação exigida para o certame ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedida de licitar e contratar com a Administração Pública do Estado do Tocantins e será descredenciada no Sistema de Cadastramento Unificado de Fornecedores (Sicaf), pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e das demais cominações legais.

10.2. Subsidiariamente, nos termos do artigo 87, da Lei nº 8.666, de 1993, pela inexecução total ou parcial das condições estabelecidas neste instrumento, o Poder Judiciário do Estado do Tocantins poderá, garantida a prévia defesa da empresa, que deverá ser apresentada no prazo de 5 (cinco) dias úteis a contar da sua notificação, aplicar, sem prejuízo das responsabilidades penal e civil, as seguintes sanções:

10.2.1. Advertência, por escrito, quando a empresa deixar de atender quaisquer indicações aqui constantes;

10.2.2. Multa compensatória/indenizatória no percentual de 5% (cinco por cento) calculado sobre o valor contratado;

10.2.3. Suspensão temporária de participação em licitação e impedimento de contratar com o Poder Judiciário do Estado do Tocantins, pelo prazo de até 2 (dois) anos; e

10.2.4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

10.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pela empresa, a esta será aplicada multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor do contrato ou instrumento equivalente, por dia de atraso, limitada a 10% (dez por cento) do valor inadimplido.

10.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhido ao Fundo Especial de Modernização e Aprimoramento do Poder Judiciário – FUNJURIS, dentro do prazo de 5 (cinco) dias úteis após a respectiva notificação.

10.5. Caso não seja paga no prazo previsto no subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado pelo Poder Judiciário do Estado do Tocantins ou cobrada judicialmente.

10.6. Além das penalidades citadas, a empresa ficará sujeita, ainda, no que couber, às demais penalidades previstas em lei.

11. FUNDAMENTAÇÃO DA CONTRATAÇÃO

11.1. Justificativa e motivação

11.1.1. O Poder Judiciário do Estado do Tocantins, por meio da Diretoria de Tecnologia da Informação, tem se empenhado no planejamento para a sustentação técnica do ambiente de Tecnologia da Informação e Comunicação e contratação dos serviços e produtos relacionados. Com base nisso, essa contratação visa adquirir licença de solução de antivírus corporativo.

11.1.2. A existência de ataques de vírus dentro da Rede deste Poder Judiciário pode causar riscos às informações e atraso na execução de tarefas devido a problemas, tais como: lentidão, perda de arquivos importantes, parada de sistemas e até a exploração de informações sigilosas.

11.1.3. O Poder Judiciário utiliza a solução de antivírus Kaspersky Endpoint Security, instalada, configurada e operante em todo seu parque tecnológico, com equipe técnica devidamente capacitada para administrar a referida solução.

11.1.4. A renovação/aquisição do antivírus, justifica-se por ser essencial para viabilizar a proteção adequada e atualizada no ambiente computacional deste Poder Judiciário, permitindo preservar os ativos corporativos (hardware, software e, sobretudo,

dados), garantindo a integridade, confiabilidade e segurança, além da continuidade das atividades da organização.

11.1.5. Atualmente este Poder Judiciário dispõe de 2.000 licenças, do Contrato nº 99/2018 e 850 licenças, do Contrato nº 128/2019, que irão expirar nos meses de setembro e novembro de 2021, respectivamente. Vale destacar que uma mudança para outro software de antivírus ocasionaria um gasto desnecessário de tempo e custos, visto que necessitaria de uma nova implantação – incluindo custos com viagens (diárias) para instalar em equipamentos no interior, por exemplo, e nova capacitação para o corpo técnico em se tratando de solução distinta.

11.1.6. Ademais, a atual solução tem atendido às necessidades deste Poder Judiciário de forma satisfatória, não registrando, até então, incidentes relevantes durante o tempo de uso da solução.

11.1.7. Por se tratar de solução imprescindível para a segurança da informação na instituição, faz-se necessária a manutenção do software sob contrato de prestação de serviço de suporte técnico e de garantia de atualização de versão.

11.1.8. O emprego desta ferramenta de segurança possibilita monitorar e controlar o tráfego de dados que circula entre as redes internas e a Internet, garantindo a segurança e o bom funcionamento dos computadores da rede local (Intranet) contra ações de vírus e, ainda, permite a implantação de uma política de prevenção de riscos.

11.1.9. Faz-se necessária, portanto, a renovação de licenças do antivírus Kaspersky Endpoint Security – Versão Business Select – pelo período de 36 (trinta e seis) meses, para prevenir a ocorrência dos eventos citados e com isso, assegurar a continuidade dos serviços prestados, uma vez que a contratação de 2.000 licenças, do Contrato nº 99/2018 e 850 licenças, do Contrato nº 128/2019, irão expirar nos meses de setembro e novembro, respectivamente. Outrossim, vislumbramos a necessidade de registrar ata para 650 licenças as quais permitirão suprir futura demanda com aumento de computadores no parque tecnológico deste Judiciário.

11.2. Objetivos e benefícios

11.2.1. Prevenir ataques de vírus e outras ameaças digitais dentro da rede deste Poder Judiciário que possam causar perda de arquivos importantes e exploração de informações sigilosas.

11.2.2. Monitorar e controlar o tráfego de dados que circulam entre as redes interna e a Internet.

11.2.3. Garantir o bom funcionamento dos computadores da rede local contra ação de vírus.

11.2.4. Garantir acesso seguro às informações armazenadas nas bases de dados do Judiciário tocantinense.

11.2.5. Administrar os computadores da rede aplicando-lhes políticas de segurança remotamente.

11.2.6. Permitir a melhoria constante da infraestrutura e governança de TIC.

11.3. Alinhamento estratégico

11.3.1. A aquisição Solução de Tecnologia da Informação e Comunicação está contemplada no Plano de Contratação de 2021 da Diretoria de Tecnologia da Informação, conforme se depreende do SEI nº 19.0.000003602-4, evento 3492556, descrita como "Licenças Antivírus" – item 45.

11.3.2. O objeto da contratação está alinhado com um dos objetivos estratégicos definidos na Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça, qual seja:

11.3.3. Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados.

11.4. Referência aos estudos preliminares

11.4.1. Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda (DOD) e Estudos Preliminares, insertos nos eventos 3546947 e 3575158, respectivamente, do processo SEI nº 21.0.000002638-4.

11.5. Relação entre a Demanda Prevista e a Contratada

11.5.1. Atualmente, há cerca de 3.055 computadores (entre desktops e notebooks) distribuídos entre Tribunal de Justiça, Comarcas, Juizados e Anexos já com a solução de segurança instalada e operante.

11.5.2. A demanda prevista consiste na renovação de 2.850 licenças que terão sua vigência expirada, sendo que outras 650 licenças excedentes visam garantir o crescimento do parque tecnológico.

11.6. Análise de Mercado de TIC

11.6.1. Atualmente existem no mercado vários fabricantes de antivírus, sendo diferenciados pela eficiência quanto à proteção. No mercado de antivírus corporativo, pode-se citar os seguintes fabricantes: Avira, Symantec, Kaspersky, McAfee, Panda, BitDefender, Trendmicro, Sophos, Eset, entre outros.

11.6.2. Também foi realizada uma pesquisa acerca de contratações similares realizadas por outras pessoas jurídicas de direito público com a finalidade de identificação de soluções semelhantes à desejada pelo Contratante.

11.6.3. Foram algumas pessoas jurídicas que buscaram realizar licitação cujo objeto é solução de antivírus: Tribunal de Justiça do Estado de Mato Grosso; Seção Judiciária do Rio Grande do Sul (TRF4); Secretaria da Fazenda e Planejamento do Estado do Tocantins; Defensoria Pública do Estado de Goiás; Governo do Estado do Ceará; Universidade Federal do Goiás; Prefeitura Municipal de Anchieta-ES.

11.7. Natureza do objeto

11.7.1. O objeto possui natureza de bem de consumo, pois se trata de licença de antivírus. É salutar que o objeto possui características comuns e usuais encontrados no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos.

11.8. Parcelamento e Adjudicação do objeto

11.8.1. No contexto desta contratação e de acordo com os requisitos levantados, verifica-se que o objeto é composto por itens, sendo um item para renovação das licenças e outro para aquisição de licenças.

11.8.2. Observa-se que a adjudicação pode ser realizada a fornecedores diversos, não havendo problema se for adjudicado a único fornecedor.

11.9. Modalidade, Tipo de Licitação e Critérios de Seleção

11.9.1. Verifica-se que o objeto pretendido é oferecido por diversos fornecedores no mercado de TIC e apresentam características padronizadas e usuais. Assim, pode-se concluir que o objeto é comum e, portanto, sugere-se como melhor opção a utilização da modalidade "Pregão".

11.9.2. As licenças de solução corporativa de antivírus têm papel essencial à continuidade das atividades deste Poder Judiciário de forma segura, será exigido atestado de capacidade técnica, nos termos da Instrução Normativa nº 9, de 20 de julho de 2018, do Tribunal de Justiça do Estado do Tocantins, uma vez que a não comprovação pode implicar na insatisfação na execução da dos serviços prestado.

11.9.3. Igualmente, o critério de habilitação busca filtrar as empresas que realmente pertencem à área de tecnologia da informação e comunicação, ou seja, do ramo do objeto que se pretende contratar, de modo a minimizar riscos para a regular execução do objeto.

11.9.4. Portanto, o atestado de capacidade técnica, quando solicitado pela Administração nas contratações realizadas pelo Poder Judiciário do Estado do Tocantins:

11.9.4.1. Poderá ser emitido por pessoa jurídica de direito público ou privado.

11.9.4.2. Terá a finalidade de comprovar que o licitante forneceu ou está fornecendo objetos e/ou prestou ou está prestando serviços satisfatoriamente, de forma compatível com o objeto da contratação.

11.9.4.3. O atestado emitido por pessoa jurídica de direito privado será assinado pelo representante legal da pessoa emitente, o qual se responsabilizará na forma da lei.

11.9.4.4. Deverá constar no atestado, no mínimo, os seguintes dados do emitente: razão social e dados para contato; e do favorecido: razão social, número do CNPJ, objeto do contrato e dados para contato.

11.9.4.5. Será admitida a somatória de atestados de capacidade técnica sempre que inexistir motivo para a exigência de atestado único, independente da época de expedição ou localidade.

11.9.4.6. Será facultada à Comissão de Licitação, ao Pregoeiro ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo, vedada a inclusão posterior de documento ou informação relevante que deveria constar originariamente da proposta.

11.10. Impacto ambiental

11.10.1. A solução de TIC que se pretende contratar diz respeito a renovação/aquisição de licenças de antivírus e se trata de um software. Neste caso não ocorrerá descarte de nenhum equipamento, com isso, não haverá impacto ao ambiente.

11.11. Conformidade Técnica e Legal

11.11.1. A contratação deve estar de acordo com a: Lei nº 8.666, de 21 de junho de 1993; Decreto nº 10.024, de 20 de setembro de 2019; e Resolução CNJ de nº 370, de 28 de janeiro de 2021.

11.12. Obrigações Contratuais

11.12.1. Da Contratada

11.12.1.1. Responsabilizar-se pela observância de Leis, Decretos, Regulamentos, Portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto do contrato, bem como, aplicáveis aos casos de subcontratação.

11.12.1.2. Atender prontamente às solicitações do Tribunal de Justiça do Estado do Tocantins no fornecimento do objeto nas quantidades e especificações deste Termo de Referência, de acordo com a necessidade desta Corte, a partir da solicitação do gestor do contrato.

11.12.1.3. Manter, durante a execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação, em conformidade com a Lei, incluindo a atualização de documentos de controle da arrecadação de tributos e contribuições federais e outras legalmente exigíveis.

11.12.1.4. Responsabilizar-se por todos os recursos e insumos necessários ao perfeito cumprimento do objeto contratado, devendo estar incluídas no preço proposto todas as despesas com materiais, insumos, seguros, impostos, taxas, encargos e demais despesas necessárias à perfeita execução do objeto.

11.12.1.5. Indicar, formalmente, preposto apto a representá-la junto ao Contratante, que deverá responder pela fiel execução do contrato.

11.12.1.6. Prestar todos os esclarecimentos técnicos que lhe forem solicitados pelo Contratante, relacionados com as características e funcionamento do objeto, inclusive em relação aos problemas detectados.

11.12.1.7. Comunicar, imediatamente, por escrito qualquer anormalidade, prestando ao Contratante os esclarecimentos julgados necessários.

11.12.1.8. Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados; treinados e qualificados para prestação dos serviços.

11.12.1.9. Manter ficha de controle do serviço, na qual serão relatadas todas as ocorrências.

11.12.1.10. Assumir inteira responsabilidade técnica e operacional, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas na prestação do objeto.

11.12.1.11. Ficar obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nas aquisições até 25% (vinte e cinco por cento) do valor inicial deste Termo de Referência, nos termos da Lei.

11.12.1.12. Não transferir a outrem, no todo ou em parte, o objeto desta prestação.

11.12.1.13. Identificar qualquer equipamento de sua posse que venha a ser utilizado nas dependências do Poder Judiciário, afixando placas de controle patrimonial, selos de segurança etc.

11.12.1.14. Reparar quaisquer danos diretamente causados ao Contratante ou a terceiros, por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da presente relação contratual, não excluindo ou reduzindo essa responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pelo Contratante.

11.12.1.15. Cumprir integralmente as exigências do Acordo de Nível de Serviço, disposto no "ANEXO C" deste Termo de Referência.

11.12.1.16. Manter sigilo sobre todo e qualquer assunto de interesse do Poder Judiciário ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa.

11.12.2. Do Contratante

11.12.2.1. Responsabilizar-se pela observância às Leis, Decretos, Regulamentos, Portarias e demais normas legais, direta e indiretamente aplicáveis ao contrato.

11.12.2.2. Receber o objeto de acordo com as disposições deste Termo de Referência.

11.12.2.3. Comunicar imediatamente a Contratada qualquer incorreção apresentada com o objeto entregue.

11.12.2.4. Acompanhar e fiscalizar a execução do Contrato.

11.12.2.5. Responsabilizar-se pela lavratura do respectivo contrato, com base nas disposições da Lei.

11.12.2.6. Assegurar os recursos orçamentários e financeiros para custear os bens adquiridos e promover os pagamentos dentro dos prazos convencionados neste Termo de Referência.

11.12.2.7. Processar e liquidar a fatura correspondente aos valores, através de Ordem Bancária.

11.12.2.8. Zelar para que durante a vigência do contrato sejam cumpridas as obrigações assumidas por parte da Contratada, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas.

12. DISPOSIÇÕES GERAIS

12.1. A proposta deverá conter as especificações do objeto de forma clara, descrevendo detalhadamente as características técnicas do produto ofertado, incluindo especificação, marca, modelo, garantia, procedência e outros elementos que de forma inequívoca identifiquem e constatem as configurações cotadas.

ANEXO "A" DO TERMO DE REFERÊNCIA

MINUTA DO TERMO DE RECEBIMENTO PROVISÓRIO DE BENS NÃO PERMANENTES

Aos _____ dias do mês de _____ do ano de _____, este(a) GESTOR(A) encerrou os trabalhos de análise para fim de RECEBIMENTO PROVISÓRIO, previsto no Contrato nº _____/_____ (ou Nota de Empenho nº _____/_____), do Processo nº _____. Assim procedendo, este Gestor conferiu o objeto apresentado e atesta o RECEBIMENTO PROVISÓRIO, sem (ou com as seguintes) ressalvas:

1. (listar as discrepâncias, quando houver)

Palmas, _____ de _____ de _____.

_____
Gestor(a)

ANEXO "B" DO TERMO DE REFERÊNCIA

MINUTA DO TERMO DE RECEBIMENTO DEFINITIVO DE BENS NÃO PERMANENTES

Aos _____ dias do mês de _____ do ano de _____, este(a) GESTOR(A), declara para os devidos fins, que recebe definitivamente, o objeto apresentado e atesta o RECEBIMENTO DEFINITIVO, do objeto previsto no Contrato nº _____/_____ (ou Nota de Empenho nº _____/_____), do Processo nº _____.

Palmas, _____ de _____ de _____.

_____
Gestor(a)

ANEXO "C" DO TERMO DE REFERÊNCIA

ACORDO DE NÍVEL DE SERVIÇO

1. Acordo de Nível de Serviço para entrega dos objetos:

Ação	Descrição	Medidas corretivas
Prazo para entrega do objeto	Até 1 (um) dia útil de atraso referente ao prazo do tópico 5.1 deste Termo de Referência.	Advertência.
	Superior a 1 (um) útil dia e inferior a 4 (quatro) dias úteis de atraso referente ao prazo do tópico 5.1 deste Termo de Referência.	Glosa de 0,1% (zero vírgula um por cento) sobre o valor total do Contrato por dia de atraso.
	A partir de 4 (quatro) dias úteis de atraso referente ao prazo do tópico 5.1 deste Termo de Referência.	Glosa de 0,1% (zero vírgula um por cento) ao dia de atraso sobre o valor total do Contrato.
Prazo	Até 2 (duas) horas de atraso referente	Advertência.

para solução de problema	aos prazos dos tópicos 3.2.2 deste Termo de Referência.	
	Superior a 2 (duas) horas de atraso referente aos prazos dos tópicos 3.2.2 deste Termo de Referência.	Glosa de 0,05% (zero vírgula zero cinco por cento) à hora de atraso sobre o valor do contrato.
Enviar empregado sem qualificação para executar os serviços contratados.		Glosa de 0,1% (zero vírgula um por cento) por ocorrência, contada a partir da terceira eventualidade, sobre o valor total do contrato.
Deixar de cumprir determinação formal ou instrução complementar do órgão fiscalizador.		Glosa de 0,3% (zero vírgula três por cento) por ocorrência.

2. É garantido à Contratada o direito de contestação dos resultados da apuração do Acordo de Nível de Serviço, bem como apresentar as justificativas que se fizerem necessárias.

3. As justificativas, desde que aceitas pelo gestor e pelo fiscal do contrato, poderão anular a incidência de glosas e advertências na aplicação do Acordo de Nível de Serviço.

4. As penalidades deste item não excluem, nem alteram as especificadas nas Sanções Administrativas.

Minuta de Ata de Registro de Preços

ANEXO - II

Processo Administrativo 21.0.000002638-4
Pregão Eletrônico – SRP Nº __/202_
Validade da Ata: 12 (doze) meses

O **TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS**, inscrito no CNPJ/MF sob o nº 25.053.190/0001-36, com sede na Praça dos Girassóis, s/nº, centro, em Palmas/TO, neste ato representado por _____, _____, brasileiro, portador do RG nº _____SSP/___ inscrito no CPF/MF sob nº. _____, residente e domiciliado nesta Capital, doravante designado **ÓRGÃO GERENCIADOR**, nos termos da Lei nº 10.520/2002, nº 12.846/2013, pela Lei Complementar nº 123/2006, pelos Decretos nº 10.024/2019, nº 7.892/2013 e nº 8.538/2015 e, subsidiariamente, pela Lei n. 8.666/1993, e demais normas legais aplicáveis, observadas as alterações posteriores introduzidas nos referidos diplomas legais, considerando a classificação das propostas e a respectiva homologação da licitação na modalidade **Pregão Eletrônico para Registro de Preços nº. ____/20__, RESOLVE** registrar os preços da empresa doravante denominada **FORNECEDOR**, nas quantidades estimadas anuais, de acordo com a classificação por ela alcançada por item, atendendo as condições previstas no Instrumento Convocatório e as constantes desta Ata de Registro de Preços, para formação do **SISTEMA DE REGISTRO DE PREÇOS – SRP**, destinado às futuras aquisições sujeitando-se as partes às normas constantes das Leis, Instrução Normativa e Decretos supracitados e em conformidade com as disposições a seguir.

CLÁUSULA PRIMEIRA – DO OBJETO:

1.1. O objeto do presente Instrumento é o registro de preços visando à renovação e a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – Versão Business Select, incluindo atualizações e suporte técnico , com o objetivo de atender as demandas do Poder Judiciário do Estado do Tocantins.

CLÁUSULA SEGUNDA – DO FORNECEDOR REGISTRADO:

2.1. Fornecedor Registrado:

Empresa:
CNPJ/MF:
Endereço:
Telefone:
Representante:
Itens:

CLÁUSULA TERCEIRA – DOS PREÇOS REGISTRADOS:

3.1. Planilha Demonstrativa de Preços:

ITEM	DESCRIÇÕES	UND.	QTDE.	VALOR UNITÁRIO	VALOR TOTAL

Valor total					

3.2. A qualquer tempo, o preço registrado poderá ser revisto em decorrência de eventual redução daqueles existentes no mercado, cabendo ao ÓRGÃO GERENCIADOR convocar o FORNECEDOR registrado para negociar o novo valor, bem como no caso de desequilíbrio-econômico financeiro poderá o FORNECEDOR solicitar revisão dos preços registrados:

3.2.1. A revisão de preços só será admitida no caso de comprovação de desequilíbrio econômico-financeiro, por meio de planilha de custos demonstrativa da majoração e após ampla pesquisa de mercado;

3.2.2. Para a concessão da revisão de preços o FORNECEDOR deverá comunicar ao ÓRGÃO GERENCIADOR, a variação dos preços, por escrito e imediatamente, com pedido justificado de revisão do preço registrado, anexando documentos comprobatórios da majoração e/ou planilha de custos;

3.2.3. Caso o ÓRGÃO GERENCIADOR já tenha emitido a nota de empenho respectiva, para que o FORNECEDOR realize o fornecimento dos objetos, e caso ainda não tenha solicitado a revisão de preços, esta não incidirá sobre o(s) pedido(s) já formalizado(s) e empenhado(s);

3.2.4. O ÓRGÃO GERENCIADOR terá o prazo de 30 (trinta) dias, a partir do recebimento do pleito, para análise dos pedidos de revisão recebidos;

3.2.5. Durante esse período o FORNECEDOR deverá efetuar o fornecimento dos objetos pelo preço registrado e no prazo ajustado, mesmo que a revisão seja julgada procedente pelo ÓRGÃO GERENCIADOR. Nesse caso, o ÓRGÃO GERENCIADOR procederá ao reforço dos valores pertinentes aos quantitativos dos objetos empenhadas após a revisão;

3.2.6. O FORNECEDOR obrigar-se-á realizar o fornecimento dos objetos pelo preço registrado caso o pedido de revisão seja julgado improcedente;

3.2.7. Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao preço praticado no mercado o ÓRGÃO GERENCIADOR convocará o FORNECEDOR visando à negociação para redução de preços e sua adequação ao praticado no mercado;

3.2.7.1. Frustrada a negociação, o FORNECEDOR será liberado do compromisso assumido;

3.2.8. Quando o preço de mercado tornar-se superior aos preços registrados e o FORNECEDOR, mediante requerimento devidamente comprovado, não puder cumprir o compromisso, o ÓRGÃO GERENCIADOR poderá liberar o FORNECEDOR da obrigação assumida, sem aplicação de penalidade, confirmando a veracidade dos motivos e comprovantes apresentados, desde que a comunicação ocorra antes do pedido de fornecimento;

3.2.9. Em qualquer hipótese, os preços decorrentes da revisão não poderão ultrapassar os praticados no mercado, mantendo-se a diferença percentual apurado entre o valor originalmente constante da proposta do FORNECEDOR é aquela vigente no mercado à época do registro – equação econômico-financeiro;

3.2.10. Será considerado preço de mercado o que for igual ou inferior à média daqueles apurados pelo ÓRGÃO GERENCIADOR para o objeto pesquisado.

CLÁUSULA QUARTA – DA VIGÊNCIA DA ATA:

4.1. A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados a partir da publicação do extrato no Diário da Justiça Eletrônico - DJE.

4.2. Esta Ata de Registro de Preços com a indicação do FORNECEDOR e Preços Registrados será divulgada no site: http://www.tjto.jus.br / (http://www.tjto.jus.br/index.php/cidadao/licitacoes) e ficará disponibilizada durante sua vigência, que será nós termos do item 4.1.

CLÁUSULA QUINTA – DA VINCULAÇÃO:

5.1. As especificações constantes nesta Ata de Registro de Preços vinculam-se aos autos nº. 21.0.000002638-4, do qual é parte integrante e complementar independentemente de transcrição.

CLÁUSULA SEXTA – DO CANCELAMENTO DO REGISTRO DE PREÇOS:

6.1. O registro do FORNECEDOR poderá ser cancelado, garantida a prévia defesa, no prazo de 5 (cinco) dias úteis, a contar do recebimento da notificação, nas seguintes hipóteses:

6.1.1. Pelo ÓRGÃO GERENCIADOR, quando:

a) O FORNECEDOR não cumprir as exigências contidas nesta Ata de Registro de Preços, Edital de Licitação e contratos firmados;

b) O FORNECEDOR der causa à rescisão administrativa, da contratação decorrente deste Registro de Preços, por um dos motivos elencados no art. 78 e seus incisos da Lei nº. 8.666/93, alterada pela Lei nº 8.883/94;

c) O FORNECEDOR não aceitar reduzir o seu preço registrado, quando este se apresentar superior ao praticado pelo mercado;

d) por razões de interesse público, devidamente fundamentadas, na forma do inciso XII, do art. 78 da Lei nº. 8.666/93, alterada pela Lei nº. 8.883/94;

6.2. A pedido do FORNECEDOR quando:

a) Mediante solicitação por escrito, comprovar estar impossibilitado de cumprir as obrigações/exigências assumidas por meio desta Ata de Registro de Preços.

6.3. O cancelamento será precedido de processo administrativo, sendo que a decisão final deverá ser fundamentada.

6.4. A comunicação do cancelamento do registro do FORNECEDOR será feita por escrito, juntando-se o comprovante de recebimento.

6.5. No caso do FORNECEDOR encontrar-se em lugar ignorado, incerto ou inacessível, a comunicação será feita por publicação, no Diário da Justiça Eletrônico - DJE, considerando-se cancelado o registro do FORNECEDOR, a partir do 5º (quinto) dia útil, a contar da publicação; e

6.6. A solicitação do FORNECEDOR para cancelamento do registro de preço, não o desobriga do fornecimento dos objetos, até a decisão final do ÓRGÃO GERENCIADOR, a qual deverá ser prolatada no prazo máximo de 30 (trinta) dias, facultado o ÓRGÃO GERENCIADOR a aplicação das penalidades previstas nesta Ata e no Instrumento convocatório, caso não aceitas as razões do pedido.

CLÁUSULA SÉTIMA – DA FORMAÇÃO DO CADASTRO DE RESERVA:

7.1. Após o encerramento da sessão e declarada a vencedora do certame, as demais licitantes poderão reduzir seus preços ao valor da proposta da licitante declarada vencedora, com vistas a formação do cadastro de reserva.

7.2. A manifestação em integrar o cadastro de reserva não altera o resultado do certame, cabendo apenas aos itens com propostas adjudicadas.

7.3. O licitante que compuser o cadastro de reserva disposto no item 7.2, será convocado em caso de cancelamento do registro de preços do 1º (primeiro) colocado, nas hipóteses previstas nos arts. 20 e 21 do Decreto n.º 7.892/13.

7.4. Se mais de um licitante manifestar interesse em compor o cadastro de reserva a que se refere o item 7.2, os mesmos serão classificados segundo a ordem da última proposta apresentada na etapa de lances, excluídos o percentual referente à margem de preferência, quando o objeto não atender o disposto no art. 3º da Lei n.º 8.666/93.

7.5. Uma vez cancelado o registro de preços nos termos do item 7.2, a autoridade competente, convocará os participantes do certame, designando o dia e hora para realização da habilitação dos fornecedores que comporão o cadastro de reserva, observados a ordem de classificação.

7.6. A recusa injustificada do fornecedor classificado em assinar a ata, dentro do prazo estabelecido no item 7.4, ensejará a aplicação de penalidades descritas no item 18 do Edital de Licitação.

7.7. A contratação formalizar-se-á mediante instrumento particular, observadas as cláusulas e condições do Edital, da Ata de Registro de Preços e da proposta vencedora.

7.8. A licitante que tenha seu preço registrado estará obrigada a cumprir todas as condições dispostas nesta Ata de Registro de Preços.

CLÁUSULA OITAVA – DA ADESÃO À ATA DE REGISTRO DE PREÇOS:

8.1. Caberá ao órgão aderente à Ata de Registro de Preços, verificar junto ao FORNECEDOR a capacidade de fornecimento dos objetos, bem como consultar o ÓRGÃO GERENCIADOR sobre a sua anuência.

8.2. Caberá ao FORNECEDOR, observadas as condições estabelecidas, optar pela aceitação do fornecimento dos objetos, desde que não venha a prejudicar as obrigações anteriormente assumidas.

8.3. Os fornecimentos adicionais não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos de cada item do instrumento convocatório e registrado nesta Ata do ÓRGÃO GERENCIADOR e dos órgãos participantes.

8.4. O quantitativo de que trata o item 8.3, não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços do ÓRGÃO GERENCIADOR e da ata de registro de preços dos órgãos participantes, independente do número de órgão não participantes que aderirem.

8.5. Realizada a contratação/aquisição da totalidade do(s) item(ns) registrados para o ÓRGÃO GERENCIADOR não será possível à adesão desta Ata por órgão ou entidade.

CLÁUSULA NONA – DA FORMA DE AQUISIÇÃO:

9.1. As aquisições dos objetos decorrentes do Registro de Preços serão realizadas de acordo com a necessidade e conveniência do ÓRGÃO GERENCIADOR, mediante a emissão de contrato ou somente de nota de empenho, conforme for o caso.

9.2. Os quantitativos dos objetos a serem fornecidos são de livre escolha do ÓRGÃO GERENCIADOR e estarão diretamente vinculados às especificidades constantes nesta Ata.

9.3. A existência de preços registrados não obriga o ÓRGÃO GERENCIADOR a adquiri-los em sua totalidade, e sim promover a aquisição de acordo com suas necessidades, obedecida à legislação pertinente, sendo assegurada ao detentor do registro a preferência em igualdade de condições.

CLÁUSULA DÉCIMA – DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS:

10.1. Renovação de licenças de solução corporativa de antivírus

10.1.1. Características Gerais:

10.1.1.1. Todas as licenças fornecidas terão validade de 36 (trinta e seis) meses para atualizações inerentes ao produto.

10.1.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

10.1.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

10.1.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para o Contratante além daquele já cotado na proposta.

10.1.2. Servidor de Administração e Console Administrativa

10.1.2.1. Compatibilidade:

10.1.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

10.1.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

10.1.2.1.3. Microsoft Windows Server 2016 x64.

10.1.2.1.4. Microsoft Windows Server 2019 x64.

10.1.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

10.1.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

10.1.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

10.1.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

10.1.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

10.1.2.2. Características:

10.1.2.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC.

10.1.2.2.2. Console deve ser baseada no modelo cliente/servidor.

10.1.2.2.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.

10.1.2.2.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.

10.1.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

10.1.2.2.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM.

10.1.2.2.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores.

10.1.2.2.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory.

10.1.2.2.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.

10.1.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

10.1.2.2.11. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada.

10.1.2.2.12. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas.

10.1.2.2.13. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas.

10.1.2.2.14. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador.

10.1.2.2.15. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle.

10.1.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

10.1.2.2.17. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus.

10.1.2.2.18. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança.

10.1.2.2.19. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede.

10.1.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

10.1.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

10.1.2.2.22. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes.

10.1.2.2.23. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

10.1.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

10.1.2.2.25. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

10.1.2.2.25.1. Nome do computador.

10.1.2.2.25.2. Nome do domínio.

10.1.2.2.25.3. Range de IP.

10.1.2.2.25.4. Sistema Operacional.

10.1.2.2.25.5. Máquina virtual.

10.1.2.2.26. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas.

10.1.2.2.27. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional.

10.1.2.2.28. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção.

10.1.2.2.29. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção.

10.1.2.2.30. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente.

10.1.2.2.31. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias etc.

10.1.2.2.32. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos.

10.1.2.2.33. Deve fornecer as seguintes informações dos computadores:

10.1.2.2.33.1. Se o antivírus está instalado.

10.1.2.2.33.2. Se o antivírus está iniciado.

10.1.2.2.33.3. Se o antivírus está atualizado.

10.1.2.2.33.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo.

10.1.2.2.33.5. Minutos/horas desde a última atualização de vacinas.

10.1.2.2.33.6. Data e horário da última verificação executada na máquina.

10.1.2.2.33.7. Versão do antivírus instalado na máquina.

10.1.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças.

10.1.2.2.33.9. Data e horário de quando a máquina foi ligada.

10.1.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina.

10.1.2.2.33.11. Nome do computador.

10.1.2.2.33.12. Domínio ou grupo de trabalho do computador.

10.1.2.2.33.13. Data e horário da última atualização de vacinas.

10.1.2.2.33.14. Sistema operacional com Service Pack.

101.1.2.2.33.15. Quantidade de processadores.

10.1.2.2.33.16. Quantidade de memória RAM.

10.1.2.2.33.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory).

10.1.2.2.33.18. Endereço IP.

10.1.2.2.33.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.

10.1.2.2.33.20. Atualizações do Windows Updates instaladas.

10.1.2.2.33.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD.

10.1.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina.

10.1.2.2.34. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las.

10.1.2.2.35. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

10.1.2.2.35.1. Alteração de Gateway Padrão.

10.1.2.2.35.2. Alteração de subrede.

2.1.2.2.35.3. Alteração de domínio.

10.1.2.2.35.4. Alteração de servidor DHCP.

10.1.2.2.35.5. Alteração de servidor DNS.

10.1.2.2.35.6. Alteração de servidor WINS.

10.1.2.2.35.7. Alteração de subrede.

10.1.2.2.35.8. Resolução de Nome.

10.1.2.2.35.9. Disponibilidade de endereço de conexão SSL.

10.1.2.2.36. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet.

10.1.2.2.37. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes.

10.1.2.2.38. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus.

10.1.2.2.39. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos.

10.1.2.2.40. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede.

10.1.2.2.41. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.

10.1.2.2.42. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

10.1.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos.

10.1.2.2.44. Capacidade de enviar e-mails para contas específicas em caso de algum evento.

10.1.2.2.45. Listar em um único local, todos os computadores não gerenciados na rede.

10.1.2.2.46. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes.

10.1.2.2.47. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

10.1.2.2.48. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação etc.), inclusive de máquinas que estejam em subnets diferentes do servidor.

10.1.2.2.49. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo).

10.1.2.2.50. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador.

10.1.2.2.51. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (exemplo: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint).

10.1.2.2.52. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação.

10.1.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

10.1.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

10.1.2.2.55. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

10.1.2.2.55.1. Nome do vírus.

10.1.2.2.55.2. Nome do arquivo infectado.

10.1.2.2.55.3. Data e hora da detecção.

10.1.2.2.55.4. Nome da máquina ou endereço IP.

10.1.2.2.55.5. Ação realizada.

10.1.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

10.1.2.2.57. Capacidade de listar updates nas máquinas com o respectivo link para download.

10.1.2.2.58. Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração.

10.1.2.2.59. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante.

10.1.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente.

10.1.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

10.1.3. Estações Windows

10.1.3.1. Compatibilidade:

10.1.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate.

10.1.3.1.2. Microsoft Windows 8 Professional/Enterprise.

10.1.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

10.1.3.1.4. Microsoft Windows 10 Professional/Enterprise.

10.1.3.2. Características:

10.1.3.2.1. Deve prover as seguintes proteções:

10.1.3.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

10.1.3.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus).

10.1.3.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos).

10.1.3.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza.

10.1.3.2.1.5. Firewall com IDS.

10.1.3.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus).

10.1.3.2.1.7. Controle de dispositivos externos.

10.1.3.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

10.1.3.2.1.9. Controle de acesso a sites por horário.

10.1.3.2.1.10. Controle de acesso a sites por usuários.

10.1.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

10.1.3.2.1.12. Controle de execução de aplicativos.

10.1.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

10.1.3.2.2.Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

10.1.3.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

10.1.3.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

10.1.3.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (exemplo: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

10.1.3.2.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas.

10.1.3.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

10.1.3.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

10.1.3.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

10.1.3.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas.

10.1.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

10.1.3.2.12. Capacidade de verificar objetos usando heurística.

10.1.3.2.13. Capacidade de agendar uma pausa na verificação.

10.1.3.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias.

10.1.3.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

10.1.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

10.1.3.2.16.1. Perguntar o que fazer, ou;

10.1.3.2.16.2. Bloquear acesso ao objeto.

10.1.3.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

10.1.3.2.16.2.2. Caso positivo de desinfecção:

10.1.3.2.16.2.2.1. Restaurar o objeto para uso.

10.1.3.2.16.2.3. Caso negativo de desinfecção:

10.1.3.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

10.1.3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

10.1.3.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI.

10.1.3.2.19. Capacidade de verificar links inseridos em e-mails contra phishings.

10.1.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

10.1.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

10.1.3.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

10.1.3.2.22.1. Perguntar o que fazer, ou;

10.1.3.2.22.2. Bloquear o e-mail.

10.1.3.2.22.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

10.1.3.2.22.2.2. Caso positivo de desinfecção:

10.1.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

10.1.3.2.22.2.3. Caso negativo de desinfecção:

10.1.3.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador).

10.1.3.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

10.1.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

10.1.3.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.

10.1.3.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script etc.), usando heurísticas.

10.1.3.2.27. Deve ter suporte total ao protocolo Ipv6.

10.1.3.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail.

10.1.3.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

10.1.3.2.29.1. Perguntar o que fazer, ou;

10.1.3.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

10.1.3.2.29.3. Permitir acesso ao objeto.

10.1.3.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

10.1.3.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

10.1.3.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

10.1.3.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

10.1.3.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.

10.1.3.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

10.1.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

10.1.3.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

10.1.3.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica.

10.1.3.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

10.1.3.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

10.1.3.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas.

10.1.3.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

10.1.3.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

10.1.3.2.39.1. Discos de armazenamento locais.

10.1.3.2.39.2. Armazenamento removível.

10.1.3.2.39.3. Impressoras.

10.1.3.2.39.4. CD/DVD.

10.1.3.2.39.5. Drives de disquete.

10.1.3.2.39.6. Modems.

10.1.3.2.39.7. Dispositivos de fita.

10.1.3.2.39.8. Dispositivos multifuncionais.

10.1.3.2.39.9. Leitores de smart card.

10.1.3.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile etc.).

10.1.3.2.39.11. Wi-Fi.

10.1.3.2.39.12. Adaptadores de rede externos.

10.1.3.2.39.13. Dispositivos MP3 ou smartphones.

10.1.3.2.39.14. Dispositivos Bluetooth.

10.1.3.2.39.15. Câmeras e Scanners.

10.1.3.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário.

10.1.3.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

10.1.3.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

10.1.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

10.1.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

10.1.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

10.1.3.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

10.1.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

10.1.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

10.1.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

10.1.3.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.

10.1.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

10.1.3.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

10.1.3.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

10.1.3.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

10.1.3.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

10.1.3.2.54. Capacidade de integração com o Windows Defender Security Center.

10.1.3.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).

10.1.3.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

10.1.4. Estações Mac OS X

10.1.4.1. Compatibilidade:

10.1.4.1.1. OS X 10.9 (Mavericks).

10.1.4.1.2. OS X 10.10 (Yosemite).

10.1.4.1.3. OS X 10.11 (El Capitan).

10.1.4.1.4. macOS 10.12 (Sierra).

10.1.4.1.5. macOS 10.13 (High Sierra).

10.1.4.1.6. macOS 10.14 (Mojave).

10.1.4.1.7. macOS 10.15 (Catalina).

10.1.4.1.8. macOS 11.0 (Big Sur).

10.1.4.2. Características:

10.1.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

10.1.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https.

10.1.4.2.3. Possuir módulo de bloqueio a ataques na rede.

10.1.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador.

10.1.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

10.1.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

10.1.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

10.1.4.2.8. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

10.1.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

10.1.4.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

10.1.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

10.1.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

10.1.4.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

10.1.4.2.14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

10.1.4.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

10.1.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

10.1.4.2.17. Capacidade de verificar objetos usando heurística.

10.1.4.2.18. Capacidade de agendar uma pausa na verificação.

10.1.4.2.19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

10.1.4.2.19.1. Perguntar o que fazer, ou;

10.1.4.2.19.2. Bloquear acesso ao objeto.

10.1.4.2.19.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

10.1.4.2.19.3.1. Caso positivo de desinfecção:

10.1.4.2.19.3.1.1. Restaurar o objeto para uso.

10.1.4.2.19.3.2. Caso negativo de desinfecção:

10.1.4.2.19.3.2.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

10.1.4.2.20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

10.1.4.2.21. Capacidade de verificar arquivos de formato de email.

10.1.4.2.22. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, parar o antivírus e iniciar o antivírus pela linha de comando.

10.1.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

10.1.5. Estações Linux

10.1.5.1. Compatibilidade:

10.1.5.1.1. Plataforma 32 bits:

10.1.5.1.1.1. Ubuntu 16.04 LTS

10.1.5.1.1.2. Red Hat® Enterprise Linux® 6.7

10.1.5.1.1.3. CentOS-6.7

10.1.5.1.1.4. Debian GNU / Linux 9.4

10.1.5.1.2. Plataforma 64 bits:

10.1.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

10.1.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

10.1.5.1.2.3. CentOS-6.7, 7.2, 8.0

10.1.5.1.2.4. Debian GNU / Linux 9.4, 10.1

10.1.5.1.2.5. OracleLinux 7.3, 8

10.1.5.1.2.6. SUSE® Linux Enterprise Server 15

10.1.5.1.2.7. openSUSE® 15

10.1.5.1.2.8. Amazon Linux AMI

10.1.5.2. Características:

10.1.5.2.1. Deve prover as seguintes proteções:

10.1.5.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

10.1.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

10.1.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

10.1.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

10.1.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

10.1.5.2.7. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

10.1.5.2.8. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

10.1.5.2.9. Capacidade de criar exclusões por local, máscara e nome da ameaça.

10.1.5.2.10. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

10.1.5.2.11. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

10.1.5.2.12. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers.

10.1.5.2.13. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

10.1.5.2.13.1. Alta.

10.1.5.2.13.2. Média.

10.1.5.2.13.3. Baixa.

10.1.5.2.13.4. Recomendado.

10.1.5.2.14. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

10.1.5.2.15. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos. desinfecção ou remoção de objetos infectados.

10.1.5.2.16. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

10.1.5.2.17. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

10.1.5.2.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

10.1.5.2.19. Capacidade de verificar objetos usando heurística.

10.1.5.2.20. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

10.1.5.2.21. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

10.1.6. Servidores Windows

10.1.6.1. Compatibilidade:

10.1.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

10.1.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

10.1.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

10.1.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

10.1.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

10.1.6.1.6. Microsoft Windows Server 2016.

10.1.6.1.7. Microsoft Windows Server 2019.

10.1.6.2. Características:

10.1.6.2.1. Deve prover as seguintes proteções:

10.1.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

10.1.6.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus.

10.1.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

10.1.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

10.1.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

10.1.6.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

10.1.6.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

10.1.6.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

10.1.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

10.1.6.2.4.3. Leitura de configurações.

10.1.6.2.4.4. Modificação de configurações.

10.1.6.2.4.5. Gerenciamento de Backup e Quarentena.

10.1.6.2.4.6. Visualização de relatórios.

10.1.6.2.4.7. Gerenciamento de relatórios.

10.1.6.2.4.8. Gerenciamento de chaves de licença.

10.1.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

10.1.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

10.1.6.2.6. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede.

10.1.6.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros etc.).

10.1.6.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS).

10.1.6.2.9. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares.

10.1.6.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

10.1.6.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.

10.1.6.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

10.1.6.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

10.1.6.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

10.1.6.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

10.1.6.2.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

10.1.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

10.1.6.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (exemplo: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários etc.).

10.1.6.2.19. Capacidade de verificar objetos usando heurística.

10.1.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

10.1.6.2.21. Capacidade de agendar uma pausa na verificação.

10.1.6.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

10.1.6.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

10.1.6.2.23.1. Perguntar o que fazer, ou;

10.1.6.2.23.2. Bloquear acesso ao objeto.

10.1.6.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

10.1.6.2.23.2.2. Caso positivo de desinfecção:

10.1.6.2.23.2.2.1. Restaurar o objeto para uso.

10.1.6.2.23.3. Caso negativo de desinfecção:

10.1.6.2.23.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

10.1.6.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

10.1.6.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

10.1.6.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

10.1.6.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

10.1.6.2.28. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

10.1.6.2.29. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

10.1.6.2.30. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

10.1.7. Servidores Linux

10.1.7.1. Compatibilidade:

10.1.7.1.1. Plataforma 32 bits:

10.1.7.1.1.1. Ubuntu 16.04 LTS.

10.1.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

10.1.7.1.1.3. CentOS-6.7.

10.1.7.1.1.4. Debian GNU / Linux 9.4.

10.1.7.1.2. Plataforma 64 bits:

10.1.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

10.1.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

10.1.7.1.2.3. CentOS-6.7, 7.2, 8.0.

10.1.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

10.1.7.1.2.5. OracleLinux 7.3, 8.

10.1.7.1.2.6. SUSE® Linux Enterprise Server 15.

10.1.7.1.2.7. openSUSE® 15.

10.1.7.1.2.8. Amazon Linux AMI.

10.1.7.2. Características:

10.1.7.2.1. Deve prover as seguintes proteções:

10.1.7.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

10.1.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

10.1.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

10.1.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

10.1.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

2.1.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

10.1.7.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

10.1.7.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

10.1.7.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

10.1.7.2.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

10.1.7.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

10.1.7.2.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

10.1.7.2.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

10.1.7.2.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

10.1.7.2.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

10.1.7.2.7. Capacidade de verificar objetos usando heurística.

10.1.7.2.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

10.1.7.2.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

10.1.7.2.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

10.1.8. Smartphones e tablets

10.1.8.1. Compatibilidade:

10.1.8.1.1. Dispositivos com os sistemas operacionais:

10.1.8.1.1.1. Android 4.2 – 11.

10.1.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

10.1.8.2. Características:

10.1.8.2.1. Deve prover as seguintes proteções:

10.1.8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

10.1.8.2.1.2. Proteção contra adware e autodialers.

10.1.8.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.

10.1.8.2.1.4. Arquivos abertos no smartphone.

10.1.8.2.1.5. Programas instalados usando a interface do smartphone

10.1.8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento.

10.1.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

10.1.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

10.1.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

10.1.8.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.

10.1.8.2.6. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha.

10.1.8.2.7. Deverá ter firewall pessoal (Android).

10.1.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

10.1.8.2.9. Capacidade de enviar comandos remotamente de:

10.1.8.2.9.1. Localizar.

10.1.8.2.9.2. Bloquear.

10.1.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

10.1.8.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos.

10.1.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

10.1.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

10.1.8.2.14. Capacidade de localizar o dispositivo quando necessário.

10.1.8.2.15. Permitir atualização das definições quando estiver em "roaming".

10.1.8.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus.

10.1.8.2.17. Deve permitir verificar somente arquivos executáveis.

10.1.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

10.1.8.2.19. Capacidade de agendar uma verificação.

10.1.8.2.20. Capacidade de enviar URL de instalação por e-mail.

10.1.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

10.1.8.2.22. Capacidade de executar as seguintes ações caso a desinfecção falhe:

10.1.8.2.22.1. Deletar.

10.1.8.2.22.2. Ignorar.

10.1.8.2.22.3. Quarentenar.

10.1.8.2.22.4. Perguntar ao usuário.

10.1.9. Gerenciamento de dispositivos móveis (MDM):

10.1.9.1. Compatibilidade:

10.1.9.1.1. Android 4.2 – 11.

10.1.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

10.1.9.2. Características:

10.1.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

10.1.9.2.2. Capacidade de ajustar as configurações de:

10.1.9.2.2.1. Sincronização de e-mail.

10.1.9.2.2..2. Uso de aplicativos.

10.1.9.2.2.3. Senha do usuário.

10.1.9.2.2.4. Criptografia de dados.

10.1.9.2.2.5. Conexão de mídia removível.

10.1.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

10.1.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

10.1.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

10.1.9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS.

10.1.9.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento.

10.1.9.2.8. Permitir sincronização com perfil do "Touch Down".

10.1.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

10.1.9.2.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual.

10.1.9.2.11. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

10.2. Aquisição de licenças de solução corporativa de antivírus

10.2.1. Características Gerais

10.2.1.1. Todas as licenças fornecidas terão validade de 36 (trinta e seis) meses para atualizações inerentes ao produto.

10.2.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

10.2.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

10.2.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para o Contratante além daquele já cotado na proposta.

10.2.2. Servidor de Administração e Console Administrativa

10.2.2.1. Compatibilidade:

10.2.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

10.2.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

10.2.2.1.3. Microsoft Windows Server 2016 x64.

10.2.2.1.4. Microsoft Windows Server 2019 x64.

10.2.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

10.2.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

10.2.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

10.2.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

10.2.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

10.2.2.2. Características:

10.2.2.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC.

10.2.2.2.2. Console deve ser baseada no modelo cliente/servidor.

10.2.2.2.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.

10.2.2.2.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.

10.2.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

10.2.2.2.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM.

10.2.2.2.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores.

10.2.2.2.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory.

10.2.2.2.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.

10.2.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

10.2.2.2.11. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada.

10.2.2.2.12. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas.

10.2.2.2.13. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas.

10.2.2.2.14. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador.

10.2.2.2.15. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle.

10.2.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

10.2.2.2.17. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus.

10.2.2.2.18. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança.

10.2.2.2.19. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede.

10.2.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

10.2.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

10.2.2.2.22. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes.

10.2.2.2.23. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

10.2.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

10.2.2.2.25. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

10.2.2.2.25.1. Nome do computador.

10.2.2.2.25.2. Nome do domínio.

10.2.2.2.25.3. Range de IP.

10.2.2.2.25.4. Sistema Operacional.

10.2.2.2.25.5. Máquina virtual.

10.2.2.2.26. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas.

10.2.2.2.27. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional.

10.2.2.2.28. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção.

10.2.2.2.29. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção.

10.2.2.2.30. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente.

10.2.2.2.31. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias etc.

10.2.2.2.32. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos.

10.2.2.2.33. Deve fornecer as seguintes informações dos computadores:

10.2.2.2.33.1. Se o antivírus está instalado.

10.2.2.2.33.2. Se o antivírus está iniciado.

10.2.2.2.33.3. Se o antivírus está atualizado.

10.2.2.2.33.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo.

10.2.2.2.33.5. Minutos/horas desde a última atualização de vacinas.

10.2.2.2.33.6. Data e horário da última verificação executada na máquina.

10.2.2.2.33.7. Versão do antivírus instalado na máquina.

10.2.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças.

10.2.2.2.33.9. Data e horário de quando a máquina foi ligada.

10.2.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina.

10.2.2.2.33.11. Nome do computador.

10.2.2.2.33.12. Domínio ou grupo de trabalho do computador.

10.2.2.2.33.13. Data e horário da última atualização de vacinas.

10.2.2.2.33.14. Sistema operacional com Service Pack.

10.2.2.2.33.15. Quantidade de processadores.

10.2.2.2.33.16. Quantidade de memória RAM.

10.2.2.2.33.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory).

10.2.2.2.33.18. Endereço IP.

10.2.2.2.33.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.

10.2.2.2.33.20. Atualizações do Windows Updates instaladas.

10.2.2.2.33.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD.

10.2.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina.

10.2.2.2.34. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las.

10.2.2.2.35. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

10.2.2.2.35.1. Alteração de Gateway Padrão.

10.2.2.2.35.2. Alteração de subrede.

10.2.2.2.35.3. Alteração de domínio.

10.2.2.2.35.4. Alteração de servidor DHCP.

10.2.2.2.35.5. Alteração de servidor DNS.

10.2.2.2.35.6. Alteração de servidor WINS.

10.2.2.2.35.7. Alteração de subrede.

10.2.2.2.35.8. Resolução de Nome.

10.2.2.2.35.9. Disponibilidade de endereço de conexão SSL.

10.2.2.2.36. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet.

10.2.2.2.37. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes.

10.2.2.2.38. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus.

10.2.2.2.39. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos.

10.2.2.2.40. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede.

10.2.2.2.41. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.

10.2.2.2.42. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

10.2.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos.

10.2.2.2.44. Capacidade de enviar e-mails para contas específicas em caso de algum evento.

10.2.2.2.45. Listar em um único local, todos os computadores não gerenciados na rede.

10.2.2.2.46. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes.

10.2.2.2.47. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

10.2.2.2.48. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação etc.), inclusive de máquinas que estejam em subnets diferentes do servidor.

10.2.2.2.49. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo).

10.2.2.2.50. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador.

10.2.2.2.51. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (exemplo: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint).

10.2.2.2.52. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação.

10.2.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

10.2.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

10.2.2.2.55. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

10.2.2.2.55.1. Nome do vírus.

10.2.2.2.55.2. Nome do arquivo infectado.

10.2.2.2.55.3. Data e hora da detecção.

10.2.2.2.55.4. Nome da máquina ou endereço IP.

10.2.2.2.55.5. Ação realizada.

10.2.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

10.2.2.2.57. Capacidade de listar updates nas máquinas com o respectivo link para download.

10.2.2.2.58. Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração.

10.2.2.2.59. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante.

10.2.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente.

10.2.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

10.2.3. Estações Windows

10.2.3.1. Compatibilidade:

10.2.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate.

10.2.3.1.2. Microsoft Windows 8 Professional/Enterprise.

10.2.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

10.2.3.1.4. Microsoft Windows 10 Professional/Enterprise.

10.2.3.2. Características:

10.2.3.2.1. Deve prover as seguintes proteções:

10.2.3.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

10.2.3.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus).

10.2.3.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos).

10.2.3.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza.

10.2.3.2.1.5. Firewall com IDS.

10.2.3.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus).

10.2.3.2.1.7. Controle de dispositivos externos.

10.2.3.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

10.2.3.2.1.9. Controle de acesso a sites por horário.

10.2.3.2.1.10. Controle de acesso a sites por usuários.

10.2.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

10.2.3.2.1.12. Controle de execução de aplicativos.

10.2.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

10.2.3.2.2.Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

10.2.3.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

10.2.3.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

10.2.3.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (exemplo: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

10.2.3.2.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas.

10.2.3.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

10.2.3.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

10.2.3.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

10.2.3.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas.

10.2.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

10.2.3.2.12. Capacidade de verificar objetos usando heurística.

10.2.3.2.13. Capacidade de agendar uma pausa na verificação.

10.2.3.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias.

10.2.3.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

10.2.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

10.2.3.2.16.1. Perguntar o que fazer, ou;

10.2.3.2.16.2. Bloquear acesso ao objeto.

10.2.3.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

10.2.3.2.16.2.2. Caso positivo de desinfecção:

10.2.3.2.16.2.2.1. Restaurar o objeto para uso.

10.2.3.2.16.2.3. Caso negativo de desinfecção:

10.2.3.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

10.2.3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

10.2.3.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI.

10.2.3.2.19. Capacidade de verificar links inseridos em e-mails contra phishings.

10.2.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

10.2.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

10.2.3.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

10.2.3.2.22.1. Perguntar o que fazer, ou;

10.2.3.2.22.2. Bloquear o e-mail.

10.2.3.2.22.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

10.2.3.2.22.2.2. Caso positivo de desinfecção:

10.2.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

10.2.3.2.22.2.3. Caso negativo de desinfecção:

10.2.3.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador).

10.2.3.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

10.2.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

10.2.3.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.

10.2.3.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script etc.), usando heurísticas.

10.2.3.2.27. Deve ter suporte total ao protocolo Ipv6.

10.2.3.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail.

10.2.3.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

10.2.3.2.29.1. Perguntar o que fazer, ou;

10.2.3.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

10.2.3.2.29.3. Permitir acesso ao objeto.

10.2.3.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

10.2.3.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

10.2.3.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

10.2.3.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

10.2.3.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.

10.2.3.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

10.2.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

10.2.3.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

10.2.3.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica.

10.2.3.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

10.2.3.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

10.2.3.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas.

10.2.3.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

10.2.3.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

10.2.3.2.39.1. Discos de armazenamento locais.

10.2.3.2.39.2. Armazenamento removível.

10.2.3.2.39.3. Impressoras.

10.2.3.2.39.4. CD/DVD.

10.2.3.2.39.5. Drives de disquete.

10.2.3.2.39.6. Modems.

10.2.3.2.39.7. Dispositivos de fita.

10.2.3.2.39.8. Dispositivos multifuncionais.

10.2.3.2.39.9. Leitores de smart card.

10.2.3.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile etc.).

10.2.3.2.39.11. Wi-Fi.

10.2.3.2.39.12. Adaptadores de rede externos.

10.2.3.2.39.13. Dispositivos MP3 ou smartphones.

10.2.3.2.39.14. Dispositivos Bluetooth.

10.2.3.2.39.15. Câmeras e Scanners.

10.2.3.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário.

10.2.3.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

10.2.3.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

10.2.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

10.2.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

10.2.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

10.2.3.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

10.2.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

10.2.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

10.2.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

10.2.3.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.

10.2.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

10.2.3.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

10.2.3.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

10.2.3.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

10.2.3.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

10.2.3.2.54. Capacidade de integração com o Windows Defender Security Center.

10.2.3.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).

10.2.3.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

10.2.4. Estações Mac OS X

10.2.4.1. Compatibilidade:

10.2.4.1.1. OS X 10.9 (Mavericks).

10.2.4.1.2. OS X 10.10 (Yosemite).

10.2.4.1.3. OS X 10.11 (El Capitan).

10.2.4.1.4. macOS 10.12 (Sierra).

10.2.4.1.5. macOS 10.13 (High Sierra).

10.2.4.1.6. macOS 10.14 (Mojave).

10.2.4.1.7. macOS 10.15 (Catalina).

10.2.4.1.8. macOS 11.0 (Big Sur).

10.2.4.2. Características:

10.2.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

10.2.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https.

10.2.4.2.3. Possuir módulo de bloqueio a ataques na rede.

10.2.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador.

10.2.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

10.2.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

10.2.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

10.2.4.2.8. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

10.2.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

10.2.4.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

10.2.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

10.2.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

10.2.4.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

10.2.4.2.14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

10.2.4.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

10.2.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

10.2.4.2.17. Capacidade de verificar objetos usando heurística.

10.2.4.2.18. Capacidade de agendar uma pausa na verificação.

10.2.4.2.19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

10.2.4.2.19.1. Perguntar o que fazer, ou;

10.2.4.2.19.2. Bloquear acesso ao objeto.

10.2.4.2.19.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

10.2.4.2.19.3.1. Caso positivo de desinfecção:

10.2.4.2.19.3.1.1. Restaurar o objeto para uso.

10.2.4.2.19.3.2. Caso negativo de desinfecção:

10.2.4.2.19.3.2.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

10.2.4.2.20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

10.2.4.2.21. Capacidade de verificar arquivos de formato de email.

10.2.4.2.22. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, parar o antivírus e iniciar o antivírus pela linha de comando.

10.2.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

10.2.5. Estações Linux

10.2.5.1. Compatibilidade:

10.2.5.1.1. Plataforma 32 bits:

10.2.5.1.1.1. Ubuntu 16.04 LTS

10.2.5.1.1.2. Red Hat® Enterprise Linux® 6.7

10.2.5.1.1.3. CentOS-6.7

10.2.5.1.1.4. Debian GNU / Linux 9.4

10.2.5.1.2. Plataforma 64 bits:

10.2.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

10.2.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

10.2.5.1.2.3. CentOS-6.7, 7.2, 8.0

10.2.5.1.2.4. Debian GNU / Linux 9.4, 10.1

10.2.5.1.2.5. OracleLinux 7.3, 8

10.2.5.1.2.6. SUSE® Linux Enterprise Server 15

10.2.5.1.2.7. openSUSE® 15

10.2.5.1.2.8. Amazon Linux AMI

10.2.5.2. Características

10.2.5.2.1. Deve prover as seguintes proteções:

10.2.5.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

10.2.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

10.2.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

10.2.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

10.2.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

10.2.5.2.7. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

10.2.5.2.8. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

10.2.5.2.9. Capacidade de criar exclusões por local, máscara e nome da ameaça.

10.2.5.2.10. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

10.2.5.2.11. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

10.2.5.2.12. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers.

10.2.5.2.13. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

10.2.5.2.13.1. Alta.

10.2.5.2.13.2. Média.

10.2.5.2.13.3. Baixa.

10.2.5.2.13.4. Recomendado.

10.2.5.2.14. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

10.2.5.2.15. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos. desinfecção ou remoção de objetos infectados.

10.2.5.2.16. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

10.2.5.2.17. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

10.2.5.2.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

10.2.5.2.19. Capacidade de verificar objetos usando heurística.

10.2.5.2.20. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

10.2.5.2.21. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

10.2.6. Servidores Windows

10.2.6.1. Compatibilidade:

10.2.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

10.2.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

10.2.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

10.2.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

10.2.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

10.2.6.1.6. Microsoft Windows Server 2016.

10.2.6.1.7. Microsoft Windows Server 2019.

10.2.6.2. Características:

10.2.6.2.1. Deve prover as seguintes proteções:

10.2.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

10.2.6.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus.

10.2.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

10.2.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

10.2.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

10.2.6.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

10.2.6.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

10.2.6.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

10.2.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

10.2.6.2.4.3. Leitura de configurações.

10.2.6.2.4.4. Modificação de configurações.

10.2.6.2.4.5. Gerenciamento de Backup e Quarentena.

10.2.6.2.4.6. Visualização de relatórios.

10.2.6.2.4.7. Gerenciamento de relatórios.

10.2.6.2.4.8. Gerenciamento de chaves de licença.

10.2.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

10.2.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

10.2.6.2.6. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede.

10.2.6.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros etc.).

10.2.6.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS).

10.2.6.2.9. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares.

10.2.6.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

10.2.6.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.

10.2.6.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

10.2.6.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

10.2.6.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

10.2.6.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

10.2.6.2.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

10.2.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

10.2.6.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (exemplo: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários etc.).

10.2.6.2.19. Capacidade de verificar objetos usando heurística.

10.2.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

10.2.6.2.21. Capacidade de agendar uma pausa na verificação.

10.2.6.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

10.2.6.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

10.2.6.2.23.1. Perguntar o que fazer, ou;

10.2.6.2.23.2. Bloquear acesso ao objeto.

10.2.6.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

10.2.6.2.23.2.2. Caso positivo de desinfecção:

10.2.6.2.23.2.2.1. Restaurar o objeto para uso.

10.2.6.2.23.3. Caso negativo de desinfecção:

10.2.6.2.23.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

10.2.6.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

10.2.6.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

10.2.6.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

10.2.6.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

10.2.6.2.28. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

10.2.6.2.29. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

10.2.6.2.30. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

10.2.7. Servidores Linux

10.2.7.1. Compatibilidade:

10.2.7.1.1. Plataforma 32 bits:

10.2.7.1.1.1. Ubuntu 16.04 LTS.

10.2.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

10.2.7.1.1.3. CentOS-6.7.

10.2.7.1.1.4. Debian GNU / Linux 9.4.

10.2.7.1.2. Plataforma 64 bits:

10.2.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

10.2.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

10.2.7.1.2.3. CentOS-6.7, 7.2, 8.0.

10.2.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

10.2.7.1.2.5. OracleLinux 7.3, 8.

10.2.7.1.2.6. SUSE® Linux Enterprise Server 15.

10.2.7.1.2.7. openSUSE® 15.

10.2.7.1.2.8. Amazon Linux AMI.

10.2.7.2. Características:

10.2.7.2.1. Deve prover as seguintes proteções:

10.2.7.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

10.2.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

10.2.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

10.2.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

10.2.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

10.2.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

10.2.7.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

10.2.7.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

10.2.7.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

10.2.7.2.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

10.2.7.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

10.2.7.2.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

10.2.7.2.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

10.2.7.2.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

10.2.7.2.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

10.2.7.2.7. Capacidade de verificar objetos usando heurística.

10.2.7.2.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

10.2.7.2.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

10.2.7.2.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

10.2.8. Smartphones e tablets

10.2.8.1. Compatibilidade:

10.2.8.1.1. Dispositivos com os sistemas operacionais:

10.2.8.1.1.1. Android 4.2 – 11.

10.2.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

10.2.8.2. Características:

10.2.8.2.1. Deve prover as seguintes proteções:

10.2.8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

10.2.8.2.1.2. Proteção contra adware e autodialers.

10.2.8.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.

10.2.8.2.1.4. Arquivos abertos no smartphone.

10.2.8.2.1.5. Programas instalados usando a interface do smartphone

10.2.8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento.

10.2.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

10.2.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

10.2.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

10.2.8.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.

10.2.8.2.6. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha.

10.2.8.2.7. Deverá ter firewall pessoal (Android).

10.2.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

10.2.8.2.9. Capacidade de enviar comandos remotamente de:

10.2.8.2.9.1. Localizar.

10.2.8.2.9.2. Bloquear.

10.2.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

10.2.8.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos.

10.2.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

10.2.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

10.2.8.2.14. Capacidade de localizar o dispositivo quando necessário.

10.2.8.2.15. Permitir atualização das definições quando estiver em "roaming".

10.2.8.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus.

10.2.8.2.17. Deve permitir verificar somente arquivos executáveis.

10.2.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

10.2.8.2.19. Capacidade de agendar uma verificação.

10.2.8.2.20. Capacidade de enviar URL de instalação por e-mail.

10.2.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

10.2.8.2.22. Capacidade de executar as seguintes ações caso a desinfecção falhe:

10.2.8.2.22.1. Deletar.

10.2.8.2.22.2. Ignorar.

10.2.8.2.22.3. Quarentenar.

10.2.8.2.22.4. Perguntar ao usuário.

10.2.9. Gerenciamento de dispositivos móveis (MDM):

10.2.9.1. Compatibilidade:

10.2.9.1.1. Android 4.2 – 11.

10.2.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

10.2.9.2. Características:

10.2.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

10.2.9.2.2. Capacidade de ajustar as configurações de:

10.2.9.2.2.1. Sincronização de e-mail.

10.2.9.2.2..2. Uso de aplicativos.

10.2.9.2.2.3. Senha do usuário.

10.2.9.2.2.4. Criptografia de dados.

10.2.9.2.2.5. Conexão de mídia removível.

10.2.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

10.2.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

10.2.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

10.2.9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS.

10.2.9.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento.

10.2.9.2.8. Permitir sincronização com perfil do "Touch Down".

10.2.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

10.2.9.2.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual.

10.2.9.2.11. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

10.3. Transferência de conhecimento e direitos de propriedade intelectual

10.3.1. O uso de uma solução de antivírus corporativo é imprescindível por conter funções de proteção que vão além de um antivírus comum, evitando, portanto, invasões ou roubos de informações, por exemplo. Por isso, não existe versões corporativas gratuitas, não sendo vislumbrada outra forma de utilização senão a obrigatoriedade da renovação/aquisição dessa tecnologia de terceiros.

10.3.2. Os antivírus corporativos são produtos consolidados no mercado de Tecnologia da Informação e Comunicação no Brasil e utilizados por organizações públicas e privadas. Desta forma, os riscos de descontinuidade desse produto no mercado parecem ser mínimos.

10.3.3. O FORNECEDOR deverá realizar a transferência de conhecimento nas versões dos softwares que serão adquiridos pelo Contratante e com isso, repassar informações de configuração, testes, procedimentos de contingência e demais informações necessárias

para a operação e manutenção da solução.

10.3.4. Não se aplica o requisito pertinente aos direitos de propriedade intelectual e autoral da STIC, uma vez que não será produzido nenhum artefato, tampouco trata de desenvolvimento de software.

CLÁUSULA DÉCIMA PRIMEIRA – DA DINÂMICA DE EXECUÇÃO:

11.1. A tabela abaixo sintetiza as etapas de execução desta contratação. O prazo em todas as etapas tem como referência inicial o fim da etapa anterior.

Etapa	Descrição	Quando ocorre
1	Recebimento do pedido de fornecimento.	O TJTO encaminhará o pedido de fornecimento a qualquer tempo dentro da vigência da Ata de Registro de Preços e após a assinatura do contrato.
2	Entrega das licenças.	O prazo será de até 20 (vinte) dias úteis, contados a partir da data de assinatura do contrato ou recebimento da nota de empenho.
3	Recebimento provisório das licenças.	Imediatamente após o recebimento das licenças, para efeito de posterior verificação da conformidade do material com a especificação, nos termos do artigo 73, da Lei nº 8.666, de 1993.
4	Avaliação das licenças entregues.	Após a entrega, será realizada uma avaliação e homologação pelos responsáveis técnicos. A análise para comprovação das características técnicas consistirá em avaliar as documentações apresentadas e também informações de registro das licenças no site oficial do fabricante.
5	Recebimento Definitivo das licenças.	O responsável técnico deverá, após a comprovação do atendimento das especificações técnicas, emitir e assinar em, no máximo, 15 (quinze) dias úteis, contados do primeiro dia útil posterior à entrega dos equipamentos, o Termo de Recebimento Definitivo, nos termos do artigo 73, da Lei nº 8.666, de 1993.
6	Início da contagem do prazo de garantia.	Data da emissão do recebimento definitivo das licenças. Se for o caso de licenças vincendas, a garantia iniciará no dia subsequente após o fim da vigência desta.
7	Fim do prazo de garantia	Após 36 (trinta e seis) meses.

CLÁUSULA DÉCIMA SEGUNDA - RECEBIMENTO:

12.1. O ÓRGÃO GERENCIADOR expedirá "Termo de Recebimento Provisório", o qual deverá ser assinado pelo gestor, no prazo de 10 (dez) dias úteis, para efeito de posterior verificação da conformidade dos objetos com as especificações constantes neste Termo de Referência, nos termos do artigo 73, II, *"a"*, da Lei nº 8.666, de 1993.

12.2. Após a verificação da qualidade e quantidade dos objetos e consequente aceitação, nos termos do artigo 73, II, *"b"*, da Lei nº 8.666, 1993, o ÓRGÃO GERENCIADOR emitirá "Termo de Recebimento Definitivo", no prazo de 10 (dez) dias úteis, o qual deverá ser assinado pelo gestor.

12.3. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança dos objetos fornecidos, nem ético-profissional, para perfeita execução do objeto, dentro dos limites estabelecidos pela lei ou pelo contrato.

12.4. O FORNECEDOR é obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

CLÁUSULA DÉCIMA TERCEIRA – DO PAGAMENTO:

13.1. O FORNECEDOR deverá, obrigatoriamente, apresentar nota fiscal correspondente aos objetos fornecidos.

13.2. Os pagamentos serão efetuados após análise da conformidade dos objetos entregues discriminado na respectiva nota fiscal e o atesto do gestor do contrato.

13.3. O atesto do gestor do contrato na nota fiscal é condição indispensável para o pagamento:

13.3.1. Na ausência do gestor do contrato (férias, licença ou em viagem por interesse do ÓRGÃO GERENCIADOR), o atesto será dado pelo gestor substituto.

13.4. O ÓRGÃO GERENCIADOR reserva-se o direito de não atestar a nota fiscal para o pagamento, se os dados constantes desta estiverem em desacordo com os dados do FORNECEDOR ou, ainda, se os objetos fornecidos não estiverem em conformidade com as especificações apresentadas neste Instrumeno e no Termo de Referência, ficando o pagamento suspenso até a regularização.

13.5. O pagamento será efetuado em até 30 (trinta) dias corridos, após o protocolo de recebimento da nota fiscal (momento em que o credor está adimplente com a obrigação firmada perante o ÓRGÃO GERENCIADOR), sendo que, recaindo sobre dias não úteis, o termo final será prorrogado para o dia útil subsequente.

13.6. O pagamento será realizado, no prazo previsto no item anterior, por meio de ordem bancária em conta corrente do FORNECEDOR, quando mantidas as mesmas condições iniciais de habilitação e caso não haja fato impeditivo para o qual não tenha concorrido.

13.7. O CNPJ constante da Nota Fiscal deverá ser o mesmo indicado na proposta e nota de empenho e vinculado à conta-corrente.

13.8. O ÓRGÃO GERENCIADOR somente pagará o FORNECEDOR o que for solicitado e entregue.

13.9. Ocorrendo atraso no pagamento, e desde que tal não tenha concorrido de alguma forma o FORNECEDOR, haverá incidência de atualização monetária sobre o valor devido, pela variação acumulada do índice Geral de Preços – Disponibilidade Interna (IGP-DI), coluna 2, publicado pela FGV, ocorrida entre a data final prevista para o pagamento e a data de sua efetiva realização.

13.10. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que o FORNECEDOR providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o ÓRGÃO GERENCIADOR.

13.11. Todos os atos inerentes ao presente processo obedecerão às regras concernentes ao Sistema de Eletrônico de Informações - SEI, do ÓRGÃO GERENCIADOR.

CLÁUSULA DÉCIMA QUARTA – DAS OBRIGAÇÕES DO ÓRGÃO GERENCIADOR:

14.1. O ÓRGÃO GERENCIADOR obriga-se a:

14.1.1. Observar as leis, decretos, regulamentos, portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto do Sistema de Registro de Preços;

14.1.2. Responsabilizar-se pela lavratura do respectivo contrato ou instrumento equivalente, com base nas disposições da Lei n°. 8.666/93 e suas alterações;

14.1.3. Receber os objetos de acordo com as disposições desta Ata e do Termo de Referência;

14.1.4. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

14.1.5. Comunicar ao FORNECEDOR, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

14.1.6. Acompanhar e fiscalizar o cumprimento das obrigações do FORNECEDOR, por meio de comissão/servidor especialmente designado;

14.1.7. Prestar quaisquer esclarecimentos que venham ser formalmente solicitados pelo FORNECEDOR e pertinente ao objeto desta Ata;

14.1.8. Zelar pelo bom andamento deste Registro de Preços dirimindo quaisquer dúvidas que porventura existam;

14.1.9. Assegurar os recursos orçamentários e financeiros para custear as aquisições decorrentes desta Ata;

14.1.10. Processar e liquidar a fatura correspondente, por meio de Ordem Bancária, desde que não haja fato impeditivo imputado ao FORNECEDOR;

14.1.11. Zelar para que durante a vigência desta Ata, bem como dos contratos firmados, que sejam cumpridas as obrigações assumidas por parte do FORNECEDOR, bem como sejam mantidas todas as condições de habilitação e qualificação exigida;

14.1.12. Gerenciar, a presente Ata indicando sempre que solicitado, o nome do FORNECEDOR, o preço registrado, os quantitativos disponíveis e as especificações dos objetos registrados, observada a ordem de classificação indicada na licitação;

14.1.13. Conduzir eventuais procedimentos administrativos de renegociação de preços registrados, para fins de adequação às novas condições de mercado, e de aplicação de penalidades.

CLÁUSULA DÉCIMA QUINTA – DAS OBRIGAÇÕES DO FORNECEDOR:

15.1. O FORNECEDOR obriga-se a:

15.1.1. Observar as leis, decretos, regulamentos, portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto do Sistema de Registro de Preços;

15.1.2. Cumprir todas as obrigações constantes neste Instrumento, no Edital, seus Anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução deste Registro de Preços;

15.1.3. Atender prontamente às solicitações do ÓRGÃO GERENCIADOR no fornecimento do objeto nas quantidades e especificações deste Termo de Referência, de acordo com a necessidade desta Corte, a partir da solicitação do gestor do contrato.

15.1.4. Responsabilizar-se por todos os recursos e insumos necessários ao perfeito cumprimento do objeto contratado, devendo estar incluídas no preço proposto todas as despesas com materiais, insumos, seguros, impostos, taxas, encargos e demais despesas necessárias à perfeita execução do objeto.

15.1.5. Indicar, formalmente, preposto apto a representá-la junto ao ÓRGÃO GERENCIADOR, que deverá responder pela fiel execução do contrato.

15.1.6. Prestar todos os esclarecimentos técnicos que lhe forem solicitados pelo Contratante, relacionados com as características e funcionamento do objeto, inclusive em relação aos problemas detectados.

15.1.7. Comunicar, imediatamente, por escrito qualquer anormalidade, prestando ao Contratante os esclarecimentos julgados necessários.

15.1.8. Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados; treinados e qualificados para prestação dos serviços.

15.1.9. Manter ficha de controle do serviço, na qual serão relatadas todas as ocorrências.

15.1.10. Assumir inteira responsabilidade técnica e operacional, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas na prestação do objeto.

15.1.11. Ficar obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nas aquisições até 25% (vinte e cinco por cento) do valor inicial deste Termo de Referência, nos termos da Lei.

15.1.12. Não transferir a outrem, no todo ou em parte, o objeto desta prestação.

15.1.13. Identificar qualquer equipamento de sua posse que venha a ser utilizado nas dependências do CONTRATANTE, afixando placas de controle patrimonial, selos de segurança etc.

15.1.14. Reparar quaisquer danos diretamente causados ao ÓRGÃO GERENCIADOR ou a terceiros, por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da presente relação contratual, não excluindo ou reduzindo essa responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pelo Contratante.

15.1.15. Cumprir integralmente as exigências do Acordo de Nível de Serviço, disposto no "ANEXO C" do Termo de Referência.

15.1.16. Manter sigilo sobre todo e qualquer assunto de interesse do ÓRGÃO GERENCIADOR ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa.

15.1.17. Manter, durante a vigência desta Ata e execução do contrato firmados, todas as condições de habilitação e qualificação exigidas na licitação, em conformidade com art. 55, inciso XIII, da Lei nº 8.666/93, incluindo a atualização de documentos de controle da arrecadação de tributos e contribuições federais e outras legalmente exigíveis.

CLÁUSULA DÉCIMA SEXTA – DA GESTÃO E FISCALIZAÇÃO:

16.1. Profissionais do FORNECEDOR: equipe composta por técnicos do FORNECEDOR, responsáveis pela execução e acompanhamento do objeto.

16.1.1. Técnico: funcionário do FORNECEDOR, responsável pela execução técnica-operacional.

16.1.2. Preposto: funcionário representante do FORNECEDOR, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

16.2. Equipe de Gestão do Contrato: equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares.

16.2.1. Gestor do Contrato: servidor responsável pela gestão contratual, conforme Decreto Judiciário nº 291, de 2009 e Portaria nº 255, de 2009, do Tribunal de Justiça do Estado do Tocantins.

16.2.2. Fiscal Demandante: servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos funcionais da solução.

16.2.3. Fiscal Técnico: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.

16.2.4. Fiscal Administrativo: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

16.3. A atuação ou a eventual omissão da Fiscalização durante a realização dos trabalhos, não poderá ser invocada para eximir o FORNECEDOR da responsabilidade no fornecimento dos produtos.

16.4. A fiscalização será sob o aspecto qualitativo e quantitativo, devendo ser anotado, em registro próprio as falhas detectadas, e comunicadas ao gestor do contrato todas as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte da Contratada.

16.5. A comunicação entre a fiscalização e o FORNECEDOR será realizada por meio de correspondência oficial e anotações ou registros no mesmo processo que tratam da aquisição dos objetos.

16.6. Quando houver necessidade o gestor deverá emitir notificações para o FORNECEDOR.

CLÁUSULA DÉCIMA SÉTIMA – DAS SANÇÕES ADMINISTRATIVAS:

17.1. O FORNECEDOR que, convocado dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar a documentação exigida ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedida de licitar e contratar com a Administração Pública do Estado do Tocantins e será descredenciada no Sistema de Cadastramento Unificado de Fornecedores (Sicaf), pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais.

17.2. Subsidiariamente, nos termos do art. 87 da Lei nº. 8.666/93, pela inexecução total ou parcial das condições estabelecidas neste Instrumento, o ÓRGÃO GERENCIADOR poderá, garantida a prévia defesa do FORNECEDOR, que deverá ser apresentada no prazo de 5 (cinco) dias úteis a contar da sua notificação, aplicar, sem prejuízo das responsabilidades penal e civil, as seguintes sanções:

a) Advertência, por escrito, quando o FORNECEDOR deixar de atender quaisquer indicações aqui constantes

b) Multa compensatória/indenizatória no percentual de 5% (cinco por cento) calculado sobre o valor contratado;

c) Suspensão temporária de participação em licitação e impedimento de contratar com o Poder Judiciário do Estado do Tocantins, pelo prazo de até 2 (dois) anos; e

d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o FORNECEDOR ressarcir o ÓRGÃO GERENCIADOR pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

17.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pelo FORNECEDOR, a este será aplicado multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor do contrato, por dia de atraso, limitada a 10% (dez por cento) do valor inadimplido.

17.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhido ao Fundo Especial de Modernização e Aprimoramento do Poder Judiciário – Funjuris, dentro do prazo de 5 (cinco) dias úteis após a respectiva notificação;

17.5. Caso não seja paga no prazo previsto no subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado pelo ÓRGÃO GERENCIADOR ou cobrada judicialmente.

17.6. Além das penalidades citadas, o FORNECEDOR ficará sujeito, ainda, no que couber, às demais penalidades referidas no Capítulo IV da Lei nº. 8.666/93.

A presente Ata, após lida e achada conforme, é assinada pelos representantes legais do ÓRGÃO GERENCIADOR e do FORNECEDOR, por meio de assinatura eletrônica, utilizando-se do Sistema Eletrônico de Informações - SEI.

Palmas - TO, ___ de _____ de 20__.

FORNECEDOR REGISTRADO
XXXXXX

ÓRGÃO GERENCIADOR
TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS
XXXXXXX

Documento assinado eletronicamente por **Solange Carvalho Bragança Milhomem, Técnico Judiciário de 2ª Instância**, em 22/06/2021, às 14:29, conforme art. 1º, III, "b", da Lei 11.419/2006.

Minuta de Contrato

ANEXO - III

CONTRATO Nº. ___/__
PREGÃO ELETRÔNICO - SRP Nº ____/202__
ATA DE REGISTRO DE PREÇOS ____/202__
PROCESSO 21.0.000002638-4

CONTRATO QUE CELEBRAM ENTRE SI O TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS E A EMPRESA _____.

Pelo presente Instrumento e na melhor forma de direito o **TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS**, inscrito no CNPJ/MF sob o nº 25.053.190/0001-36, com sede na Praça dos Girassóis, s/nº, centro, Palmas/TO, neste ato representado por _____, brasileiro, casado, portador do RG nº. _____ – SSP/____, inscrito no CPF/MF sob o nº. _____, residente e domiciliado nesta Capital, doravante designado **CONTRATANTE** e, do outro lado, a empresa _____ _____, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº _____, com sede _____, doravante designada **CONTRATADA**, neste ato representada por _____, portador do RG nº _____, inscrito no CPF/MF sob o nº _____, têm entre si, justo e avençado o presente Contrato, observadas as disposições da Lei nº 10.520/2002 e, subsidiariamente pela Lei 8.666/93, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO:

1.1. O presente Instrumento tem por objeto a renovação e a aquisição de licença de solução corporativa de antivírus Kaspersky Endpoint Security – Versão Business Select, incluindo atualizações e suporte técnico, com o objetivo de atender as demandas do Poder Judiciário do Estado do Tocantins, conforme descrição e quantitativos abaixo:

ITEM	DESCRIÇÃO	QTDE.	UND.	VALOR UNITÁRIO	VALOR TOTAL
Valor total					

1.2. A aquisição citada na subcláusula 1.1 obedecerá ao estipulado neste Contrato, bem como as especificações técnicas, forma de execução/entrega e as disposições dos documentos adiante enumerados, constantes do Processo Administrativo do 21.0.000002638-4 e _____, do CONTRATANTE, e que, independentemente de transcrição, fazem parte integrante e complementar deste, no que não o contrariarem. São eles:

1.2.1. O Edital do Pregão Eletrônico - SRP nº ___/202_, do CONTRATANTE; e

1.2.2. A Ata de Registro de Preços nº __/202___, resultado do Pregão Eletrônico – SRP nº ____/202___.

1.2.3. A Proposta de Preços e documentos que o acompanham, firmada pela CONTRATADA em ___ de _____ de 202_.

1.3. A aquisição do objeto deste Contrato foi realizada por meio de procedimento licitatório, de acordo com o disposto no art. 1º e parágrafo único e art. 2º parágrafo 1º da Lei nº 10.520/2002, sob a modalidade Pregão, na forma eletrônica, para registro de preços, conforme Edital e Processo Administrativo acima citados.

1.4. A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

1.5. Nenhum acréscimo poderá exceder os limites estabelecidos no item anterior, salvo as supressões que poderão exceder os limites legais, quando acordadas entre as Partes.

CLÁUSULA SEGUNDA – DA FORMALIZAÇÃO DO CONTRATO:

2.1. A empresa será convocada para assinatura do instrumento contratual, devendo assiná-lo e restituí-lo no prazo de 5 (cinco) dias corridos, podendo este prazo ser prorrogado, a critério do CONTRATANTE, por igual período e por uma vez, desde que ocorra motivo justificado:

2.1.1. A assinatura deste Contrato será realizada por meio eletrônica, utilizando-se do Sistema Eletrônico de Informações - SEI/TJTO.

2.3. No ato de assinatura deste Contrato, a empresa deverá atender as disposições da Portaria n° 97/2010, quanto à verificação da regularidade fiscal. Se qualquer das certidões apresentadas na fase de habilitação do procedimento licitatório expirar sua validade antes da data de assinatura deste Instrumento ou de seus aditivos, deverá a mesma ser atualizada.

CLÁUSULA TERCEIRA – DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS:

3.1. Renovação de licenças de solução corporativa de antivírus

2.1.1. Características Gerais:

3.1.1.1. Todas as licenças fornecidas terão validade de 36 (trinta e seis) meses para atualizações inerentes ao produto.

3.1.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

3.1.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

3.1.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para o Contratante além daquele já cotado na proposta.

3.1.2. Servidor de Administração e Console Administrativa

3.1.2.1. Compatibilidade:

3.1.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

3.1.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

3.1.2.1.3. Microsoft Windows Server 2016 x64.

3.1.2.1.4. Microsoft Windows Server 2019 x64.

3.1.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

3.1.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

3.1.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

3.1.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

3.1.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

3.1.2.2. Características:

3.1.2.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC.

3.1.2.2.2. Console deve ser baseada no modelo cliente/servidor.

3.1.2.2.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.

3.1.2.2.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.

3.1.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

3.1.2.2.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM.

3.1.2.2.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores.

3.1.2.2.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory.

3.1.2.2.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.

3.1.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

3.1.2.2.11. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada.

3.1.2.2.12. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas.

3.1.2.2.13. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas.

3.1.2.2.14. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador.

3.1.2.2.15. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle.

3.1.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

3.1.2.2.17. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus.

3.1.2.2.18. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança.

3.1.2.2.19. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede.

3.1.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

3.1.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

3.1.2.2.22. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes.

3.1.2.2.23. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

2.1.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

3.1.2.2.25. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

3.1.2.2.25.1. Nome do computador.

3.1.2.2.25.2. Nome do domínio.

3.1.2.2.25.3. Range de IP.

3.1.2.2.25.4. Sistema Operacional.

3.1.2.2.25.5. Máquina virtual.

3.1.2.2.26. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas.

3.1.2.2.27. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional.

3.1.2.2.28. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção.

3.1.2.2.29. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção.

3.1.2.2.30. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente.

3.1.2.2.31. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias etc.

3.1.2.2.32. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos.

3.1.2.2.33. Deve fornecer as seguintes informações dos computadores:

3.1.2.2.33.1. Se o antivírus está instalado.

3.1.2.2.33.2. Se o antivírus está iniciado.

3.1.2.2.33.3. Se o antivírus está atualizado.

3.1.2.2.33.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo.

3.1.2.2.33.5. Minutos/horas desde a última atualização de vacinas.

3.1.2.2.33.6. Data e horário da última verificação executada na máquina.

3.1.2.2.33.7. Versão do antivírus instalado na máquina.

3.1.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças.

3.1.2.2.33.9. Data e horário de quando a máquina foi ligada.

3.1.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina.

3.1.2.2.33.11. Nome do computador.

3.1.2.2.33.12. Domínio ou grupo de trabalho do computador.

3.1.2.2.33.13. Data e horário da última atualização de vacinas.

3.1.2.2.33.14. Sistema operacional com Service Pack.

3.1.2.2.33.15. Quantidade de processadores.

3.1.2.2.33.16. Quantidade de memória RAM.

3.1.2.2.33.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory).

3.1.2.2.33.18. Endereço IP.

3.1.2.2.33.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.

3.1.2.2.33.20. Atualizações do Windows Updates instaladas.

3.1.2.2.33.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD.

3.1.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina.

3.1.2.2.34. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las.

3.1.2.2.35. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

3.1.2.2.35.1. Alteração de Gateway Padrão.

3.1.2.2.35.2. Alteração de subrede.

3.1.2.2.35.3. Alteração de domínio.

3.1.2.2.35.4. Alteração de servidor DHCP.

3.1.2.2.35.5. Alteração de servidor DNS.

3.1.2.2.35.6. Alteração de servidor WINS.

3.1.2.2.35.7. Alteração de subrede.

3.1.2.2.35.8. Resolução de Nome.

3.1.2.2.35.9. Disponibilidade de endereço de conexão SSL.

3.1.2.2.36. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet.

3.1.2.2.37. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes.

3.1.2.2.38. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus.

3.1.2.2.39. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos.

3.1.2.2.40. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede.

3.1.2.2.41. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.

3.1.2.2.42. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

3.1.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos.

3.1.2.2.44. Capacidade de enviar e-mails para contas específicas em caso de algum evento.

3.1.2.2.45. Listar em um único local, todos os computadores não gerenciados na rede.

3.1.2.2.46. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes.

3.1.2.2.47. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente.

3.1.2.2.48. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação etc.), inclusive de máquinas que estejam em subnets diferentes do servidor.

3.1.2.2.49. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo).

3.1.2.2.50. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador.

3.1.2.2.51. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (exemplo: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint).

3.1.2.2.52. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação.

3.1.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

3.1.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

3.1.2.2.55. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

3.1.2.2.55.1. Nome do vírus.

3.1.2.2.55.2. Nome do arquivo infectado.

3.1.2.2.55.3. Data e hora da detecção.

3.1.2.2.55.4. Nome da máquina ou endereço IP.

3.1.2.2.55.5. Ação realizada.

3.1.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

3.1.2.2.57. Capacidade de listar updates nas máquinas com o respectivo link para download.

3.1.2.2.58. Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração.

3.1.2.2.59. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante.

3.1.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente.

3.1.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

3.1.3. Estações Windows

3.1.3.1. Compatibilidade:

3.1.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate.

3.1.3.1.2. Microsoft Windows 8 Professional/Enterprise.

3.1.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

3.1.3.1.4. Microsoft Windows 10 Professional/Enterprise.

3.1.3.2. Características:

3.1.3.2.1. Deve prover as seguintes proteções:

3.1.3.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

3.1.3.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus).

3.1.3.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos).

3.1.3.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza.

3.1.3.2.1.5. Firewall com IDS.

3.1.3.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus).

3.1.3.2.1.7. Controle de dispositivos externos.

3.1.3.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

3.1.3.2.1.9. Controle de acesso a sites por horário.

3.1.3.2.1.10. Controle de acesso a sites por usuários.

3.1.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

3.1.3.2.1.12. Controle de execução de aplicativos.

3.1.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

3.1.3.2.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

3.1.3.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

3.1.3.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

3.1.3.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (exemplo: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

3.1.3.2.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas.

3.1.3.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

3.1.3.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

3.1.3.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

3.1.3.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas.

3.1.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

3.1.3.2.12. Capacidade de verificar objetos usando heurística.

3.1.3.2.13. Capacidade de agendar uma pausa na verificação.

3.1.3.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias.

3.1.3.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

3.1.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

3.1.3.2.16.1. Perguntar o que fazer, ou;

3.1.3.2.16.2. Bloquear acesso ao objeto.

3.1.3.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

3.1.3.2.16.2.2. Caso positivo de desinfecção:

3.1.3.2.16.2.2.1. Restaurar o objeto para uso.

3.1.3.2.16.2.3. Caso negativo de desinfecção:

3.1.3.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

3.1.3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

3.1.3.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI.

3.1.3.2.19. Capacidade de verificar links inseridos em e-mails contra phishings.

3.1.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

3.1.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

3.1.3.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

3.1.3.2.22.1. Perguntar o que fazer, ou;

3.1.3.2.22.2. Bloquear o e-mail.

3.1.3.2.22.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

3.1.3.2.22.2.2. Caso positivo de desinfecção:

3.1.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

3.1.3.2.22.2.3. Caso negativo de desinfecção:

3.1.3.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador).

3.1.3.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

3.1.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

3.1.3.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.

3.1.3.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script etc.), usando heurísticas.

3.1.3.2.27. Deve ter suporte total ao protocolo Ipv6.

3.1.3.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail.

3.1.3.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

3.1.3.2.29.1. Perguntar o que fazer, ou;

3.1.3.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

3.1.3.2.29.3. Permitir acesso ao objeto.

3.1.3.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

3.1.3.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

3.1.3.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

3.1.3.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

3.1.3.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.

3.1.3.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

3.1.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

3.1.3.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

3.1.3.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica.

3.1.3.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

3.1.3.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

3.1.3.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas.

3.1.3.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.1.3.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

3.1.3.2.39.1. Discos de armazenamento locais.

3.1.3.2.39.2. Armazenamento removível.

3.1.3.2.39.3. Impressoras.

3.1.3.2.39.4. CD/DVD.

3.1.3.2.39.5. Drives de disquete.

3.1.3.2.39.6. Modems.

3.1.3.2.39.7. Dispositivos de fita.

3.1.3.2.39.8. Dispositivos multifuncionais.

3.1.3.2.39.9. Leitores de smart card.

3.1.3.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile etc.).

3.1.3.2.39.11. Wi-Fi.

3.1.3.2.39.12. Adaptadores de rede externos.

3.1.3.2.39.13. Dispositivos MP3 ou smartphones.

3.1.3.2.39.14. Dispositivos Bluetooth.

3.1.3.2.39.15. Câmeras e Scanners.

3.1.3.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário.

3.1.3.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

3.1.3.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

3.1.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

3.1.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

3.1.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

3.1.3.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

3.1.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

3.1.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

3.1.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

3.1.3.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.

3.1.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

3.1.3.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

3.1.3.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

3.1.3.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

3.1.3.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

3.1.3.2.54. Capacidade de integração com o Windows Defender Security Center.

3.1.3.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).

3.1.3.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

3.1.4. Estações Mac OS X

3.1.4.1. Compatibilidade:

3.1.4.1.1. OS X 10.9 (Mavericks).

3.1.4.1.2. OS X 10.10 (Yosemite).

3.1.4.1.3. OS X 10.11 (El Capitan).

3.1.4.1.4. macOS 10.12 (Sierra).

3.1.4.1.5. macOS 10.13 (High Sierra).

3.1.4.1.6. macOS 10.14 (Mojave).

3.1.4.1.7. macOS 10.15 (Catalina).

3.1.4.1.8. macOS 11.0 (Big Sur).

3.1.4.2. Características:

3.1.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

3.1.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https.

3.1.4.2.3. Possuir módulo de bloqueio a ataques na rede.

3.1.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador.

3.1.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

3.1.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

3.1.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

3.1.4.2.8. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

3.1.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

3.1.4.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

3.1.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

3.1.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

3.1.4.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

3.1.4.2.14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

3.1.4.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

3.1.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

3.1.4.2.17. Capacidade de verificar objetos usando heurística.

3.1.4.2.18. Capacidade de agendar uma pausa na verificação.

3.1.4.2.19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

3.1.4.2.19.1. Perguntar o que fazer, ou;

3.1.4.2.19.2. Bloquear acesso ao objeto.

3.1.4.2.19.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

3.1.4.2.19.3.1. Caso positivo de desinfecção:

3.1.4.2.19.3.1.1. Restaurar o objeto para uso.

3.1.4.2.19.3.2. Caso negativo de desinfecção:

3.1.4.2.19.3.2.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

3.1.4.2.20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

3.1.4.2.21. Capacidade de verificar arquivos de formato de email.

3.1.4.2.22. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, parar o antivírus e iniciar o antivírus pela linha de comando.

3.1.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

3.1.5. Estações Linux

3.1.5.1. Compatibilidade:

3.1.5.1.1. Plataforma 32 bits:

3.1.5.1.1.1. Ubuntu 16.04 LTS

3.1.5.1.1.2. Red Hat® Enterprise Linux® 6.7

3.1.5.1.1.3. CentOS-6.7

3.1.5.1.1.4. Debian GNU / Linux 9.4

3.1.5.1.2. Plataforma 64 bits:

3.1.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

3.1.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

3.1.5.1.2.3. CentOS-6.7, 7.2, 8.0

3.1.5.1.2.4. Debian GNU / Linux 9.4, 10.1

3.1.5.1.2.5. OracleLinux 7.3, 8

3.1.5.1.2.6. SUSE® Linux Enterprise Server 15

3.1.5.1.2.7. openSUSE® 15

3.1.5.1.2.8. Amazon Linux AMI

3.1.5.2. Características:

3.1.5.2.1. Deve prover as seguintes proteções:

3.1.5.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

3.1.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

3.1.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

3.1.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

3.1.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

3.1.5.2.7. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

3.1.5.2.8. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

3.1.5.2.9. Capacidade de criar exclusões por local, máscara e nome da ameaça.

3.1.5.2.10. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

3.1.5.2.11. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

3.1.5.2.12. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers.

3.1.5.2.13. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

3.1.5.2.13.1. Alta.

3.1.5.2.13.2. Média.

3.1.5.2.13.3. Baixa.

3.1.5.2.13.4. Recomendado.

3.1.5.2.14. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

3.1.5.2.15. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos. desinfecção ou remoção de objetos infectados.

3.1.5.2.16. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

3.1.5.2.17. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

3.1.5.2.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

3.1.5.2.19. Capacidade de verificar objetos usando heurística.

3.1.5.2.20. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

3.1.5.2.21. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

3.1.6. Servidores Windows

3.1.6.1. Compatibilidade:

3.1.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

3.1.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

3.1.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

3.1.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

3.1.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

3.1.6.1.6. Microsoft Windows Server 2016.

3.1.6.1.7. Microsoft Windows Server 2019.

3.1.6.2. Características:

3.1.6.2.1. Deve prover as seguintes proteções:

3.1.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

3.1.6.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus.

3.1.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

3.1.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

3.1.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

3.1.6.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

3.1.6.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

3.1.6.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

3.1.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

3.1.6.2.4.3. Leitura de configurações.

3.1.6.2.4.4. Modificação de configurações.

3.1.6.2.4.5. Gerenciamento de Backup e Quarentena.

3.1.6.2.4.6. Visualização de relatórios.

3.1.6.2.4.7. Gerenciamento de relatórios.

3.1.6.2.4.8. Gerenciamento de chaves de licença.

3.1.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

3.1.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que

podem ser executados no total.

3.1.6.2.6. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede.

3.1.6.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros etc.).

3.1.6.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS).

3.1.6.2.9. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares.

3.1.6.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

3.1.6.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.

3.1.6.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

3.1.6.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

3.1.6.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

3.1.6.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

3.1.6.2.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

3.1.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

3.1.6.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (exemplo: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários etc.).

3.1.6.2.19. Capacidade de verificar objetos usando heurística.

3.1.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

3.1.6.2.21. Capacidade de agendar uma pausa na verificação.

3.1.6.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

3.1.6.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

3.1.6.2.23.1. Perguntar o que fazer, ou;

3.1.6.2.23.2. Bloquear acesso ao objeto.

3.1.6.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

3.1.6.2.23.2.2. Caso positivo de desinfecção:

3.1.6.2.23.2.2.1. Restaurar o objeto para uso.

3.1.6.2.23.3. Caso negativo de desinfecção:

3.1.6.2.23.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

3.1.6.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

3.1.6.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

3.1.6.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

3.1.6.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

3.1.6.2.28. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros .

3.1.6.2.29. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

3.1.6.2.30. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

3.1.7. Servidores Linux

3.1.7.1. Compatibilidade:

3.1.7.1.1. Plataforma 32 bits:

3.1.7.1.1.1. Ubuntu 16.04 LTS.

3.1.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

3.1.7.1.1.3. CentOS-6.7.

3.1.7.1.1.4. Debian GNU / Linux 9.4.

3.1.7.1.2. Plataforma 64 bits:

3.1.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

3.1.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

3.1.7.1.2.3. CentOS-6.7, 7.2, 8.0.

3.1.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

3.1.7.1.2.5. OracleLinux 7.3, 8.

3.1.7.1.2.6. SUSE® Linux Enterprise Server 15.

3.1.7.1.2.7. openSUSE® 15.

3.1.7.1.2.8. Amazon Linux AMI.

3.1.7.2. Características:

3.1.7.2.1. Deve prover as seguintes proteções:

3.1.7.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

3.1.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

3.1.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

3.1.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

2.1.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

3.1.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

3.1.7.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

3.1.7.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

3.1.7.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

3.1.7.2.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

3.1.7.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

3.1.7.2.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

3.1.7.2.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

3.1.7.2.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

3.1.7.2.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

3.1.7.2.7. Capacidade de verificar objetos usando heurística.

3.1.7.2.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

3.1.7.2.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

3.1.7.2.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

3.1.8. Smartphones e tablets

3.1.8.1. Compatibilidade:

3.1.8.1.1. Dispositivos com os sistemas operacionais:

3.1.8.1.1.1. Android 4.2 – 11.

3.1.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

3.1.8.2. Características:

3.1.8.2.1. Deve prover as seguintes proteções:

3.1.8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

3.1.8.2.1.2. Proteção contra adware e autodialers.

3.1.8.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.

3.1.8.2.1.4. Arquivos abertos no smartphone.

3.1.8.2.1.5. Programas instalados usando a interface do smartphone

3.1.8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento.

3.1.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

3.1.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

3.1.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

3.1.8.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.

3.1.8.2.6. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha.

3.1.8.2.7. Deverá ter firewall pessoal (Android).

3.1.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

3.1.8.2.9. Capacidade de enviar comandos remotamente de:

3.1.8.2.9.1. Localizar.

3.1.8.2.9.2. Bloquear.

3.1.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

3.1.8.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos.

3.1.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

3.1.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

3.1.8.2.14. Capacidade de localizar o dispositivo quando necessário.

3.1.8.2.15. Permitir atualização das definições quando estiver em "roaming".

3.1.8.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus.

3.1.8.2.17. Deve permitir verificar somente arquivos executáveis.

3.1.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

3.1.8.2.19. Capacidade de agendar uma verificação.

3.1.8.2.20. Capacidade de enviar URL de instalação por e-mail.

3.1.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

3.1.8.2.22. Capacidade de executar as seguintes ações caso a desinfecção falhe:

3.1.8.2.22.1. Deletar.

3.1.8.2.22.2. Ignorar.

3.1.8.2.22.3. Quarentenar.

3.1.8.2.22.4. Perguntar ao usuário.

3.1.9. Gerenciamento de dispositivos móveis (MDM):

3.1.9.1. Compatibilidade:

3.1.9.1.1. Android 4.2 – 11.

3.1.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

3.1.9.2. Características:

3.1.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

3.1.9.2.2. Capacidade de ajustar as configurações de:

3.1.9.2.2.1. Sincronização de e-mail.

3.1.9.2.2..2. Uso de aplicativos.

3.1.9.2.2.3. Senha do usuário.

3.1.9.2.2.4. Criptografia de dados.

3.1.9.2.2.5. Conexão de mídia removível.

3.1.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

3.1.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

3.1.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

3.1.9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS.

3.1.9.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento.

3.1.9.2.8. Permitir sincronização com perfil do "Touch Down".

3.1.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

3.1.9.2.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual.

3.1.9.2.11. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

3.2. Aquisição de licenças de solução corporativa de antivírus

3.2.1. Características Gerais

3.2.1.1. Todas as licenças fornecidas terão validade de 36 (trinta e seis) meses para atualizações inerentes ao produto.

3.2.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software.

3.2.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software.

3.2.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para o Contratante além daquele já cotado na proposta.

3.2.2. Servidor de Administração e Console Administrativa

3.2.2.1. Compatibilidade:

3.2.2.1.1. Microsoft Windows Server 2012 (todas edições x64).

3.2.2.1.2. Microsoft Windows Server 2012 R2 (todas edições x64).

3.2.2.1.3. Microsoft Windows Server 2016 x64.

3.2.2.1.4. Microsoft Windows Server 2019 x64.

3.2.2.1.5. Microsoft Windows 8 Professional / Enterprise x64.

3.2.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32.

3.2.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64.

3.2.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32).

3.2.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

3.2.2.2. Características:

3.2.2.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC.

3.2.2.2.2. Console deve ser baseada no modelo cliente/servidor.

3.2.2.2.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.

3.2.2.2.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.

3.2.2.2.5. Deve permitir incluir usuários do AD para logarem no console de administração.

3.2.2.2.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM.

3.2.2.2.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores.

3.2.2.2.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory.

3.2.2.2.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.

3.2.2.2.10. Deve armazenar histórico das alterações feitas em políticas.

3.2.2.2.11. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada.

3.2.2.2.12. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas.

3.2.2.2.13. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas.

3.2.2.2.14. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador.

3.2.2.2.15. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle.

3.2.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.

3.2.2.2.17. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus.

3.2.2.2.18. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança.

3.2.2.2.19. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede.

3.2.2.2.20. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto.

3.2.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

3.2.2.2.22. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes.

3.2.2.2.23. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

3.2.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

3.2.2.2.25. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

3.2.2.2.25.1. Nome do computador.

3.2.2.2.25.2. Nome do domínio.

3.2.2.2.25.3. Range de IP.

3.2.2.2.25.4. Sistema Operacional.

3.2.2.2.25.5. Máquina virtual.

3.2.2.2.26. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas.

3.2.2.2.27. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional.

3.2.2.2.28. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção.

3.2.2.2.29. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção.

3.2.2.2.30. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente.

3.2.2.2.31. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias etc.

3.2.2.2.32. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos.

3.2.2.2.33. Deve fornecer as seguintes informações dos computadores:

3.2.2.2.33.1. Se o antivírus está instalado.

3.2.2.2.33.2. Se o antivírus está iniciado.

3.2.2.2.33.3. Se o antivírus está atualizado.

3.2.2.2.33.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo.

3.2.2.2.33.5. Minutos/horas desde a última atualização de vacinas.

3.2.2.2.33.6. Data e horário da última verificação executada na máquina.

3.2.2.2.33.7. Versão do antivírus instalado na máquina.

3.2.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças.

3.2.2.2.33.9. Data e horário de quando a máquina foi ligada.

3.2.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina.

3.2.2.2.33.11. Nome do computador.

3.2.2.2.33.12. Domínio ou grupo de trabalho do computador.

3.2.2.2.33.13. Data e horário da última atualização de vacinas.

3.2.2.2.33.14. Sistema operacional com Service Pack.

3.2.2.2.33.15. Quantidade de processadores.

3.2.2.2.33.16. Quantidade de memória RAM.

3.2.2.2.33.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory).

3.2.2.2.33.18. Endereço IP.

3.2.2.2.33.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.

3.2.2.2.33.20. Atualizações do Windows Updates instaladas.

3.2.2.2.33.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD.

3.2.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina.

3.2.2.2.34. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las.

3.2.2.2.35. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

3.2.2.2.35.1. Alteração de Gateway Padrão.

3.2.2.2.35.2. Alteração de subrede.

3.2.2.2.35.3. Alteração de domínio.

3.2.2.2.35.4. Alteração de servidor DHCP.

3.2.2.2.35.5. Alteração de servidor DNS.

3.2.2.2.35.6. Alteração de servidor WINS.

3.2.2.2.35.7. Alteração de subrede.

3.2.2.2.35.8. Resolução de Nome.

3.2.2.2.35.9. Disponibilidade de endereço de conexão SSL.

3.2.2.2.36. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet.

3.2.2.2.37. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes.

3.2.2.2.38. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus.

3.2.2.2.39. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos.

3.2.2.2.40. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede.

3.2.2.2.41. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.

3.2.2.2.42. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

3.2.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos.

3.2.2.2.44. Capacidade de enviar e-mails para contas específicas em caso de algum evento.

3.2.2.2.45. Listar em um único local, todos os computadores não gerenciados na rede.

3.2.2.2.46. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes.

3.2.2.2.47. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

3.2.2.2.48. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação etc.), inclusive de máquinas que estejam em subnets diferentes do servidor.

3.2.2.2.49. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo).

3.2.2.2.50. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador.

3.2.2.2.51. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (exemplo: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint).

3.2.2.2.52. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação.

3.2.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

3.2.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

3.2.2.2.55. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

3.2.2.2.55.1. Nome do vírus.

3.2.2.2.55.2. Nome do arquivo infectado.

3.2.2.2.55.3. Data e hora da detecção.

3.2.2.2.55.4. Nome da máquina ou endereço IP.

3.2.2.2.55.5. Ação realizada.

3.2.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

3.2.2.2.57. Capacidade de listar updates nas máquinas com o respectivo link para download.

3.2.2.2.58. Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração.

3.2.2.2.59. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante.

3.2.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente.

3.2.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

3.2.3. Estações Windows

3.2.3.1. Compatibilidade:

3.2.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate.

3.2.3.1.2. Microsoft Windows 8 Professional/Enterprise.

3.2.3.1.3. Microsoft Windows 8.1 Professional/Enterprise.

3.2.3.1.4. Microsoft Windows 10 Professional/Enterprise.

3.2.3.2. Características:

3.2.3.2.1. Deve prover as seguintes proteções:

3.2.3.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

3.2.3.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus).

3.2.3.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos).

3.2.3.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza.

3.2.3.2.1.5. Firewall com IDS.

3.2.3.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus).

3.2.3.2.1.7. Controle de dispositivos externos.

3.2.3.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

3.2.3.2.1.9. Controle de acesso a sites por horário.

3.2.3.2.1.10. Controle de acesso a sites por usuários.

3.2.3.2.1.11. Controle de acesso a websites por dados, exemplo: Bloquear websites com conteúdos de vídeo e áudio.

3.2.3.2.1.12. Controle de execução de aplicativos.

3.2.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

3.2.3.2.2.Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

3.2.3.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

3.2.3.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

3.2.3.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (exemplo: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

3.2.3.2.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas.

3.2.3.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

3.2.3.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

3.2.3.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

3.2.3.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas.

3.2.3.2.11. Capacidade de verificar somente arquivos novos e alterados.

3.2.3.2.12. Capacidade de verificar objetos usando heurística.

3.2.3.2.13. Capacidade de agendar uma pausa na verificação.

3.2.3.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias.

3.2.3.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

3.2.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

3.2.3.2.16.1. Perguntar o que fazer, ou;

3.2.3.2.16.2. Bloquear acesso ao objeto.

3.2.3.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

3.2.3.2.16.2.2. Caso positivo de desinfecção:

3.2.3.2.16.2.2.1. Restaurar o objeto para uso.

3.2.3.2.16.2.3. Caso negativo de desinfecção:

3.2.3.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

3.2.3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

3.2.3.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI.

3.2.3.2.19. Capacidade de verificar links inseridos em e-mails contra phishings.

3.2.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

3.2.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

3.2.3.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

3.2.3.2.22.1. Perguntar o que fazer, ou;

3.2.3.2.22.2. Bloquear o e-mail.

3.2.3.2.22.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

3.2.3.2.22.2.2. Caso positivo de desinfecção:

3.2.3.2.22.2.2.1. Restaurar o e-mail para o usuário.

3.2.3.2.22.2.3. Caso negativo de desinfecção:

3.2.3.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador).

3.2.3.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

3.2.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

3.2.3.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.

3.2.3.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script etc.), usando heurísticas.

3.2.3.2.27. Deve ter suporte total ao protocolo Ipv6.

3.2.3.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail.

3.2.3.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

3.2.3.2.29.1. Perguntar o que fazer, ou;

3.2.3.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

3.2.3.2.29.3. Permitir acesso ao objeto.

3.2.3.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

3.2.3.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

3.2.3.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

3.2.3.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

3.2.3.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.

3.2.3.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

3.2.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

3.2.3.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

3.2.3.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica.

3.2.3.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

3.2.3.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

3.2.3.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas.

3.2.3.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.2.3.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

3.2.3.2.39.1. Discos de armazenamento locais.

3.2.3.2.39.2. Armazenamento removível.

3.2.3.2.39.3. Impressoras.

3.2.3.2.39.4. CD/DVD.

3.2.3.2.39.5. Drives de disquete.

3.2.3.2.39.6. Modems.

3.2.3.2.39.7. Dispositivos de fita.

3.2.3.2.39.8. Dispositivos multifuncionais.

3.2.3.2.39.9. Leitores de smart card.

3.2.3.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile etc.).

3.2.3.2.39.11. Wi-Fi.

3.2.3.2.39.12. Adaptadores de rede externos.

3.2.3.2.39.13. Dispositivos MP3 ou smartphones.

3.2.3.2.39.14. Dispositivos Bluetooth.

3.2.3.2.39.15. Câmeras e Scanners.

3.2.3.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário.

3.2.3.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

3.2.3.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

3.2.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos etc.

3.2.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

3.2.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.).

3.2.3.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

3.2.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

3.2.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

3.2.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

3.2.3.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.

3.2.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

3.2.3.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

3.2.3.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

3.2.3.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

3.2.3.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

3.2.3.2.54. Capacidade de integração com o Windows Defender Security Center.

3.2.3.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).

3.2.3.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

3.2.4. Estações Mac OS X

3.2.4.1. Compatibilidade:

3.2.4.1.1. OS X 10.9 (Mavericks).

3.2.4.1.2. OS X 10.10 (Yosemite).

3.2.4.1.3. OS X 10.11 (El Capitan).

3.2.4.1.4. macOS 10.12 (Sierra).

3.2.4.1.5. macOS 10.13 (High Sierra).

3.2.4.1.6. macOS 10.14 (Mojave).

3.2.4.1.7. macOS 10.15 (Catalina).

3.2.4.1.8. macOS 11.0 (Big Sur).

3.2.4.2. Características:

3.2.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

3.2.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https.

3.2.4.2.3. Possuir módulo de bloqueio a ataques na rede.

3.2.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador.

3.2.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

3.2.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos etc.

3.2.4.2.7. Possibilidade de importar uma chave no pacote de instalação.

3.2.4.2.8. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

3.2.4.2.9. Deve possuir suportes a notificações utilizando o Growl.

3.2.4.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

3.2.4.2.11. Capacidade de voltar para a base de dados de vacina anterior.

3.2.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

3.2.4.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

3.2.4.2.14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

3.2.4.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

3.2.4.2.16. Capacidade de verificar somente arquivos novos e alterados.

3.2.4.2.17. Capacidade de verificar objetos usando heurística.

3.2.4.2.18. Capacidade de agendar uma pausa na verificação.

3.2.4.2.19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

3.2.4.2.19.1. Perguntar o que fazer, ou;

3.2.4.2.19.2. Bloquear acesso ao objeto.

3.2.4.2.19.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

3.2.4.2.19.3.1. Caso positivo de desinfecção:

3.2.4.2.19.3.1.1. Restaurar o objeto para uso.

3.2.4.2.19.3.2. Caso negativo de desinfecção:

3.2.4.2.19.3.2.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

3.2.4.2.20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

3.2.4.2.21. Capacidade de verificar arquivos de formato de email.

3.2.4.2.22. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, parar o antivírus e iniciar o antivírus pela linha de comando.

3.2.4.2.23. Capacidade de ser instalado, removido e administrado pela mesmo console central de gerenciamento.

3.2.5. Estações Linux

3.2.5.1. Compatibilidade:

3.2.5.1.1. Plataforma 32 bits:

3.2.5.1.1.1. Ubuntu 16.04 LTS

3.2.5.1.1.2. Red Hat® Enterprise Linux® 6.7

3.2.5.1.1.3. CentOS-6.7

3.2.5.1.1.4. Debian GNU / Linux 9.4

3.2.5.1.2. Plataforma 64 bits:

3.2.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

3.2.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

3.2.5.1.2.3. CentOS-6.7, 7.2, 8.0

3.2.5.1.2.4. Debian GNU / Linux 9.4, 10.1

3.2.5.1.2.5. OracleLinux 7.3, 8

3.2.5.1.2.6. SUSE® Linux Enterprise Server 15

3.2.5.1.2.7. openSUSE® 15

3.2.5.1.2.8. Amazon Linux AMI

3.2.5.2. Características

3.2.5.2.1. Deve prover as seguintes proteções:

3.2.5.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

3.2.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

3.2.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

3.2.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

3.2.5.2.7. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

3.2.5.2.8. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

3.2.5.2.9. Capacidade de criar exclusões por local, máscara e nome da ameaça.

3.2.5.2.10. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

3.2.5.2.11. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

3.2.5.2.12. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers.

3.2.5.2.13. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

3.2.5.2.13.1. Alta.

3.2.5.2.13.2. Média.

3.2.5.2.13.3. Baixa.

3.2.5.2.13.4. Recomendado.

3.2.5.2.14. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

3.2.5.2.15. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos. desinfecção ou remoção de objetos infectados.

3.2.5.2.16. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

3.2.5.2.17. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

3.2.5.2.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

3.2.5.2.19. Capacidade de verificar objetos usando heurística.

3.2.5.2.20. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

3.2.5.2.21. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

3.2.6. Servidores Windows

3.2.6.1. Compatibilidade:

3.2.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1.

3.2.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2.

3.2.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2.

3.2.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64.

3.2.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64.

3.2.6.1.6. Microsoft Windows Server 2016.

3.2.6.1.7. Microsoft Windows Server 2019.

3.2.6.2. Características:

3.2.6.2.1. Deve prover as seguintes proteções:

3.2.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

3.2.6.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus.

3.2.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a atividade de rede do computador atacante.

3.2.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

3.2.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

3.2.6.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

3.2.6.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

3.2.6.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

3.2.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

3.2.6.2.4.3. Leitura de configurações.

3.2.6.2.4.4. Modificação de configurações.

3.2.6.2.4.5. Gerenciamento de Backup e Quarentena.

3.2.6.2.4.6. Visualização de relatórios.

3.2.6.2.4.7. Gerenciamento de relatórios.

3.2.6.2.4.8. Gerenciamento de chaves de licença.

3.2.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

2.2.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

3.2.6.2.6. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede.

3.2.6.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros etc.).

3.2.6.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS).

3.2.6.2.9. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares.

3.2.6.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

3.2.6.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.

3.2.6.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

3.2.6.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

3.2.6.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

3.2.6.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

3.2.6.2.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

3.2.6.2.17. Capacidade de verificar somente arquivos novos e alterados.

3.2.6.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (exemplo: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários etc.).

3.2.6.2.19. Capacidade de verificar objetos usando heurística.

3.2.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

3.2.6.2.21. Capacidade de agendar uma pausa na verificação.

3.2.6.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

3.2.6.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

3.2.6.2.23.1. Perguntar o que fazer, ou;

3.2.6.2.23.2. Bloquear acesso ao objeto.

3.2.6.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

3.2.6.2.23.2.2. Caso positivo de desinfecção:

3.2.6.2.23.2.2.1. Restaurar o objeto para uso.

3.2.6.2.23.3. Caso negativo de desinfecção:

3.2.6.2.23.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

3.2.6.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

3.2.6.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

3.2.6.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

3.2.6.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

3.2.6.2.28. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

3.2.6.2.29. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

3.2.6.2.30. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

3.2.7. Servidores Linux

3.2.7.1. Compatibilidade:

3.2.7.1.1. Plataforma 32 bits:

3.2.7.1.1.1. Ubuntu 16.04 LTS.

3.2.7.1.1.2. Red Hat® Enterprise Linux® 6.7.

3.2.7.1.1.3. CentOS-6.7.

3.2.7.1.1.4. Debian GNU / Linux 9.4.

3.2.7.1.2. Plataforma 64 bits:

3.2.7.1.2.1. Ubuntu 16.04 e 18.04 LTS.

3.2.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0.

3.2.7.1.2.3. CentOS-6.7, 7.2, 8.0.

3.2.7.1.2.4. Debian GNU / Linux 9.4, 10.1.

3.2.7.1.2.5. OracleLinux 7.3, 8.

3.2.7.1.2.6. SUSE® Linux Enterprise Server 15.

3.2.7.1.2.7. openSUSE® 15.

3.2.7.1.2.8. Amazon Linux AMI.

3.2.7.2. Características:

3.2.7.2.1. Deve prover as seguintes proteções:

3.2.7.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware etc.) que verifique qualquer arquivo criado, acessado ou modificado.

3.2.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos.

3.2.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede.

3.2.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento.

3.2.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota.

3.2.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados.

3.2.7.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

3.2.7.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

3.2.7.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

3.2.7.2.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

3.2.7.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

3.2.7.2.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

3.2.7.2.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

3.2.7.2.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

3.2.7.2.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

3.2.7.2.7. Capacidade de verificar objetos usando heurística.

3.2.7.2.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

3.2.7.2.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

3.2.7.2.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

3.2.8. Smartphones e tablets

3.2.8.1. Compatibilidade:

3.2.8.1.1. Dispositivos com os sistemas operacionais:

3.2.8.1.1.1. Android 4.2 – 11.

3.2.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS.

3.2.8.2. Características:

3.2.8.2.1. Deve prover as seguintes proteções:

3.2.8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

3.2.8.2.1.2. Proteção contra adware e autodialers.

3.2.8.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.

3.2.8.2.1.4. Arquivos abertos no smartphone.

3.2.8.2.1.5. Programas instalados usando a interface do smartphone

3.2.8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento.

3.2.8.2.2. Deverá isolar em área de quarentena os arquivos infectados.

3.2.8.2.3. Deverá atualizar as bases de vacinas de modo agendado.

3.2.8.2.4. Capacidade de desativar por política: Wi-Fi, Câmera, Bluetooth.

3.2.8.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.

3.2.8.2.6. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha.

3.2.8.2.7. Deverá ter firewall pessoal (Android).

3.2.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente.

3.2.8.2.9. Capacidade de enviar comandos remotamente de:

3.2.8.2.9.1. Localizar.

3.2.8.2.9.2. Bloquear.

3.2.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS.

3.2.8.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos.

3.2.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso.

3.2.8.2.13. Capacidade de configurar White e blacklist de aplicativos.

3.2.8.2.14. Capacidade de localizar o dispositivo quando necessário.

3.2.8.2.15. Permitir atualização das definições quando estiver em "roaming".

3.2.8.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus.

3.2.8.2.17. Deve permitir verificar somente arquivos executáveis.

3.2.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível.

3.2.8.2.19. Capacidade de agendar uma verificação.

3.2.8.2.20. Capacidade de enviar URL de instalação por e-mail.

3.2.8.2.21. Capacidade de fazer a instalação através de um link QRCode.

3.2.8.2.22. Capacidade de executar as seguintes ações caso a desinfecção falhe:

3.2.8.2.22.1. Deletar.

3.2.8.2.22.2. Ignorar.

3.2.8.2.22.3. Quarentenar.

3.2.8.2.22.4. Perguntar ao usuário.

3.2.9. Gerenciamento de dispositivos móveis (MDM):

3.2.9.1. Compatibilidade:

3.2.9.1.1. Android 4.2 – 11.

3.2.9.1.2. iOS 10.0 – 14.0 ou iPadOS.

3.2.9.2. Características:

3.2.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

3.2.9.2.2. Capacidade de ajustar as configurações de:

3.2.9.2.2.1. Sincronização de e-mail.

3.2.9.2.2..2. Uso de aplicativos.

3.2.9.2.2.3. Senha do usuário.

3.2.9.2.2.4. Criptografia de dados.

3.2.9.2.2.5. Conexão de mídia removível.

3.2.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

3.2.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

3.2.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

3.2.9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS.

3.2.9.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento.

3.2.9.2.8. Permitir sincronização com perfil do "Touch Down".

3.2.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

3.2.9.2.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual.

3.2.9.2.11. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

3.3. Transferência de conhecimento e direitos de propriedade intelectual

3.3.1. O uso de uma solução de antivírus corporativo é imprescindível por conter funções de proteção que vão além de um antivírus comum, evitando, portanto, invasões ou roubos de informações, por exemplo. Por isso, não existe versões corporativas gratuitas, não sendo vislumbrada outra forma de utilização senão a obrigatoriedade da renovação/aquisição dessa tecnologia de terceiros.

3.3.2. Os antivírus corporativos são produtos consolidados no mercado de Tecnologia da Informação e Comunicação no Brasil e utilizados por organizações públicas e privadas. Desta forma, os riscos de descontinuidade desse produto no mercado parecem ser mínimos.

3.3.3. A CONTRATADA deverá realizar a transferência de conhecimento nas versões dos softwares que serão adquiridos pelo Contratante e com isso, repassar informações de configuração, testes, procedimentos de contingência e demais informações necessárias para a operação e manutenção da solução.

3.3.4. Não se aplica o requisito pertinente aos direitos de propriedade intelectual e autoral da STIC, uma vez que não será produzido nenhum artefato, tampouco trata de desenvolvimento de software.

CLÁUSULA QUARTA – DA DINÂMICA DE EXECUÇÃO

4.1. A tabela abaixo sintetiza as etapas de execução desta contratação. O prazo em todas as etapas tem como referência inicial o fim da etapa anterior.

Etapa	Descrição	Quando ocorre
1	Recebimento do pedido de fornecimento.	O TJTO encaminhará o pedido de fornecimento a qualquer tempo dentro da vigência da Ata de Registro de Preços e após a assinatura do contrato.
2	Entrega das licenças.	O prazo será de até 20 (vinte) dias úteis, contados a partir da data de assinatura do contrato ou recebimento da nota de empenho.

3	Recebimento provisório das licenças.	Imediatamente após o recebimento das licenças, para efeito de posterior verificação da conformidade do material com a especificação, nos termos do artigo 73, da Lei nº 8.666, de 1993.
4	Avaliação das licenças entregues.	Após a entrega, será realizada uma avaliação e homologação pelos responsáveis técnicos. A análise para comprovação das características técnicas consistirá em avaliar as documentações apresentadas e também informações de registro das licenças no site oficial do fabricante.
5	Recebimento Definitivo das licenças.	O responsável técnico deverá, após a comprovação do atendimento das especificações técnicas, emitir e assinar em, no máximo, 15 (quinze) dias úteis, contados do primeiro dia útil posterior à entrega dos equipamentos, o Termo de Recebimento Definitivo, nos termos do artigo 73, da Lei nº 8.666, de 1993.
6	Início da contagem do prazo de garantia.	Data da emissão do recebimento definitivo das licenças. Se for o caso de licenças vincendas, a garantia iniciará no dia subsequente após o fim da vigência desta.
7	Fim do prazo de garantia	Após 36 (trinta e seis) meses.

CLÁUSULA QUINTA - DO VALOR:

5.1. O valor global do presente Instrumento é de **R$** _____ (_____), compreendendo todas as despesas e custos diretos e indiretos necessários à perfeita execução deste Contrato.

CLÁUSULA SEXTA – DA DOTAÇÃO ORÇAMENTÁRIA:

6.1. A despesa com a execução do objeto deste Contrato correrá à conta da Dotação Orçamentária consignada:

Unidade Gestora:
Classificação Orçamentária:
Natureza da Despesa:
Fonte do Recurso:

6.2. As despesas inerentes à execução deste Contrato serão liquidadas por meio da Nota de Empenho que será emitida à conta da dotação orçamentária especificada nesta Cláusula.

6.3. **A CONTRATADA emitirá Nota Fiscal em observância à unidade gestora emissora da nota de empenho que albergou a aquisição.**

CLÁUSULA SÉTIMA – DO PAGAMENTO:

7.1. A CONTRATADA deverá, obrigatoriamente, apresentar nota fiscal correspondente aos objetos fornecidos.

7.2. Os pagamentos serão efetuados após análise da conformidade dos objetos entregues discriminado na respectiva nota fiscal e o atesto do gestor do contrato.

7.3. O atesto do gestor do contrato na nota fiscal é condição indispensável para o pagamento:

7.3.1. Na ausência do gestor do contrato (férias, licença ou em viagem por interesse do CONTRATANTE), o atesto será dado pelo gestor substituto.

7.4. O CONTRATANTE reserva-se o direito de não atestar a nota fiscal para o pagamento, se os dados constantes desta estiverem em desacordo com os dados da CONTRATADA ou, ainda, se os objetos fornecidos não estiverem em conformidade com as especificações apresentadas neste Instrumeno e no Termo de Referência, ficando o pagamento suspenso até a regularização.

7.5. O pagamento será efetuado em até 30 (trinta) dias corridos, após o protocolo de recebimento da nota fiscal (momento em que o credor está adimplente com a obrigação firmada perante o CONTRATANTE), sendo que, recaindo sobre dias não úteis, o termo final será prorrogado para o dia útil subsequente.

7.6. O pagamento será realizado, no prazo previsto no item anterior, por meio de ordem bancária em conta corrente da CONTRATADA: Banco _____, Agência nº _____, Conta Corrente _____, quando mantidas as mesmas

condições iniciais de habilitação e caso não haja fato impeditivo para o qual não tenha concorrido.

7.7. O CNPJ constante da Nota Fiscal deverá ser o mesmo indicado na proposta e nota de empenho e vinculado à conta-corrente.

7.8. O CONTRATANTE somente pagará à CONTRATADA o que for solicitado e entregue.

7.9. Ocorrendo atraso no pagamento, e desde que tal não tenha concorrido de alguma forma à CONTRATADA, haverá incidência de atualização monetária sobre o valor devido, pela variação acumulada do índice Geral de Preços – Disponibilidade Interna (IGP-DI), coluna 2, publicado pela FGV, ocorrida entre a data final prevista para o pagamento e a data de sua efetiva realização.

7.10. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

7.11. Todos os atos inerentes ao presente processo obedecerão às regras concernentes ao Sistema Eletrônico de Informações – SEI do CONTRATANTE.

CLÁUSULA OITAVA – DO REAJUSTE E ALTERAÇÕES:

8.1. O valor contratado é fixo e irreajustável.

8.2. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA:

9.1. A CONTRATADA obriga-se a:

9.1.1. Observar as leis, decretos, regulamentos, portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto deste Contrato;

9.1.2. Cumprir todas as obrigações constantes neste Instrumento, no Edital, seus Anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução deste Contrato;

9.1.3. Atender prontamente às solicitações do CONTRATANTE no fornecimento do objeto nas quantidades e especificações deste Termo de Referência, de acordo com a necessidade desta Corte, a partir da solicitação do gestor do contrato.

9.1.4. Responsabilizar-se por todos os recursos e insumos necessários ao perfeito cumprimento do objeto contratado, devendo estar incluídas no preço proposto todas as despesas com materiais, insumos, seguros, impostos, taxas, encargos e demais despesas necessárias à perfeita execução do objeto.

9.1.5. Indicar, formalmente, preposto apto a representá-la junto ao CONTRATANTE, que deverá responder pela fiel execução do contrato.

9.1.6. Prestar todos os esclarecimentos técnicos que lhe forem solicitados pelo Contratante, relacionados com as características e funcionamento do objeto, inclusive em relação aos problemas detectados.

9.1.7. Comunicar, imediatamente, por escrito qualquer anormalidade, prestando ao Contratante os esclarecimentos julgados necessários.

9.1.8. Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados; treinados e qualificados para prestação dos serviços.

9.1.9. Manter ficha de controle do serviço, na qual serão relatadas todas as ocorrências.

9.1.10. Assumir inteira responsabilidade técnica e operacional, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas na prestação do objeto.

9.1.11. Ficar obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nas aquisições até 25% (vinte e cinco por cento) do valor inicial deste Termo de Referência, nos termos da Lei.

9.1.12. Não transferir a outrem, no todo ou em parte, o objeto desta prestação.

9.1.13. Identificar qualquer equipamento de sua posse que venha a ser utilizado nas dependências do CONTRATANTE, afixando placas de controle patrimonial, selos de segurança etc.

9.1.14. Reparar quaisquer danos diretamente causados ao CONTRATANTE ou a terceiros, por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da presente relação contratual, não excluindo ou reduzindo essa responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pelo Contratante.

9.1.15. Cumprir integralmente as exigências do Acordo de Nível de Serviço, disposto no "ANEXO C" do Termo de Referência.

9.1.16. Manter sigilo sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa.

9.1.17. Manter, durante a execução deste Contrato, todas as condições de habilitação e qualificação exigidas na licitação, em conformidade com art. 55, inciso XIII, da Lei nº 8.666/93, incluindo a atualização de documentos de controle da arrecadação de tributos e contribuições federais e outras legalmente exigíveis.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DO CONTRATANTE:

10.1. O CONTRATANTE obriga-se a:

10.1.1. Observar as leis, decretos, regulamentos, portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto deste Contrato;

10.1.2. Responsabilizar-se pela lavratura do respectivo contrato ou instrumento equivalente, com base nas disposições da Lei n°. 8.666/93 e suas alterações;

10.1.3. Receber os objetos de acordo com as disposições deste Contrato e do Termo de Referência;

10.1.4. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

10.1.5. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

10.1.6. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, por meio de comissão/servidor especialmente designado;

10.1.8. Prestar quaisquer esclarecimentos que venham ser formalmente solicitados pelo FORNECEDOR e pertinente ao objeto desta Ata;

10.1.9. Zelar pelo bom andamento da presente aquisição/contratação, dirimindo quaisquer dúvidas que porventura existam;

10.1.10. Assegurar os recursos orçamentários e financeiros para custear a execução deste Contrato.

10.1.11. Processar e liquidar a fatura correspondente, por meio de Ordem Bancária, desde que não haja fato impeditivo imputado à CONTRATADA;

10.1.12. Zelar para que durante a vigência deste Contrato sejam cumpridas as obrigações assumidas por parte da CONTRATADA, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas.

CLÁUSULA DÉCIMA PRIMEIRA – SANÇÕES ADMINISTRATIVAS:

11.1. A CONTRATADA que, convocada dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar a documentação exigida ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedida de licitar e contratar com a Administração Pública do Estado do Tocantins e será descredenciada no Sistema de Cadastramento Unificado de Fornecedores (Sicaf), pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais;

11.2. Subsidiariamente, nos termos do art. 87 da Lei n°. 8.666/93, pela inexecução total ou parcial das condições estabelecidas neste Instrumento, o CONTRATANTE poderá, garantida a prévia defesa da CONTRATADA, que deverá ser apresentada no prazo de 5 (cinco) dias úteis a contar da sua notificação, aplicar, sem prejuízo das responsabilidades penal e civil, as seguintes sanções:

a) Advertência, por escrito, quando a CONTRATADA deixar de atender quaisquer indicações aqui constantes;

b) Multa compensatória/indenizatória no percentual de 5% (cinco por cento) calculado sobre o valor contratado;

c) Suspensão temporária de participação em licitação e impedimento de contratar com o Poder Judiciário do Estado do Tocantins, pelo prazo de até 2 (dois) anos; e

d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

11.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pela CONTRATADA, a esta será aplicada multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor deste Contrato, por dia de atraso, limitada a 10% (dez por cento) do valor inadimplido;

11.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhido ao Fundo Especial de Modernização e Aprimoramento do Poder Judiciário - Funjuris, dentro do prazo de 5 (cinco) dias úteis após a respectiva notificação;

11.5. Caso não seja paga no prazo previsto no subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado pelo Poder Judiciário do Estado do Tocantins ou cobrada judicialmente;

11.6. Além das penalidades citadas, a CONTRATADA ficará sujeita, ainda, no que couber, às demais penalidades referidas no Capítulo IV da Lei nº. 8.666/93.

CLÁUSULA DÉCIMA SEGUNDA – DA RESCISÃO:

12.1. O presente Instrumento poderá ser rescindido:

a) Por ato unilateral e escrito da Administração, nos casos enumerados nos incisos I a XII e XVII e XVIII do art. 78, da Lei 8.666/93;

b) Amigavelmente, por acordo entre as partes, reduzido a termo no respectivo procedimento administrativo, desde que haja conveniência para a Administração; ou

c) Judicialmente, nos termos da Lei.

Parágrafo Único – No caso de rescisão amigável, a parte que pretender rescindir o Contrato comunicará sua intenção à outra, por escrito.

12.2. A CONTRATADA reconhece os direitos do CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993:

12.2.1. A inexecução total ou parcial deste Contrato ensejará a sua rescisão, com às consequências estabelecidas neste Instrumento e as previstas em lei.

CLÁUSULA DÉCIMA TERCEIRA – DA VINCULAÇÃO:

13.1. O presente Contrato fica vinculado aos autos 21.0.000002638-4 e _____.

CLÁUSULA DÉCIMA QUARTA – DA LEGISLAÇÃO E CASOS OMISSOS:

14.1. O presente Instrumento, inclusive os casos omissos, regula-se pela Lei nº 10.520/2002, pelo Decreto nº 10.024/2019 e, subsidiariamente, pela Lei nº 8.666/1993 e suas alterações posteriores.

CLÁUSULA DÉCIMA QUINTA – DA VIGÊNCIA:

15.1. O presente Contrato terá vigência de 36 (trinta e seis) meses, contados a partir do recebimento definitivo da solução adquirida.

CLÁUSULA DÉCIMA SEXTA – DAS VEDAÇÕES:

16.1. É vedado à CONTRATADA:

16.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

16.1.2. Subcontratar, no todo ou em parte, a execução do objeto deste Contrato, sem anuência do CONTRATANTE;

16.1.3. Interromper a execução contratual sob alegação de inadimplemento por parte do CONTRATANTE, salvo nos casos previstos em lei.

CLÁUSULA DÉCIMA SÉTIMA – DA PUBLICAÇÃO:

17.1. A publicação resumida do presente Contrato no Diário da Justiça - DJE, que é condição indispensável para sua eficácia, será providenciada pelo CONTRATANTE, nos termos do parágrafo único do artigo 61 de Lei nº 8.666/93.

CLÁUSULA DÉCIMA OITAVA – DA GESTÃO E FISCALIZAÇÃO:

18.1. Profissionais da CONTRATADA: equipe composta por técnicos da CONTRATADA, responsáveis pela execução e acompanhamento do objeto.

18.1.1. Técnico: funcionário da CONTRATADA, responsável pela execução técnica-operacional.

18.1.2. Preposto: funcionário representante da CONTRATADA, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

18.2. Equipe de Gestão do Contrato: equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares.

18.2.1. Gestor do Contrato: servidor responsável pela gestão contratual, conforme Decreto Judiciário nº 291, de 2009 e Portaria nº 255, de 2009, do Tribunal de Justiça do Estado do Tocantins.

18.2.2. Fiscal Demandante: servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos funcionais da solução.

18.2.3. Fiscal Técnico: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.

18.2.4. Fiscal Administrativo: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

18.3. A atuação ou a eventual omissão da Fiscalização durante a realização dos trabalhos, não poderá ser invocada para eximir a CONTRATADA da responsabilidade no fornecimento dos produtos.

18.4. A fiscalização será sob o aspecto qualitativo e quantitativo, devendo ser anotado, em registro próprio as falhas detectadas, e comunicadas ao gestor do contrato todas as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte da CONTRATADA.

18.5. A comunicação entre a fiscalização e a CONTRATADA será realizada por meio de correspondência oficial e anotações ou registros no mesmo processo que tratam da aquisição dos objetos.

18.6. Quando houver necessidade o gestor deverá emitir notificações para a CONTRATADA.

CLÁUSULA DÉCIMA NONA – DAS CONDIÇÕES GERAIS:

19.1. O CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA de seus empregados, prepostos ou subordinados.

CLÁUSULA VIGÉSIMA – DO FORO:

20.1. Para dirimir todas as questões oriundas da execução do presente Contrato fica eleito o Foro de Palmas - TO, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

E, para firmeza e como prova de assim haverem, entre si, ajustado e contratado, firmam este Contrato, para que surta seus efeitos legais, por meio de assinatura eletrônica, utilizando-se do Sistema Eletrônico de Informações - SEI.

Palmas - TO, _____ de _____ de 202_.

EMPRESA CONTRATADA
xxxxxxxx
Representante legal

TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS
xxxxxxx

ANEXO - IV

MINUTA – PORTARIA DE DESIGNAÇÃO DE GESTOR DO CONTRATO

O DIRETOR GERAL DO TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS, no uso de suas atribuições legais,

CONSIDERANDO o disposto no art. 67, §§ 1º e 2º da Lei nº 8.666, de 21 de junho de 1993;

CONSIDERANDO a necessidade de acompanhar e monitorar a execução de contratos celebrados entre o Tribunal de Justiça Tocantinense e fornecedores de bens e/ou serviços;

CONSIDERANDO, ainda, o contrato nº _____/202__, referente ao Processo Administrativo _____, celebrado por este Tribunal de Justiça e a empresa _____, que tem por objeto _____, com o objetivo de atender as demandas do Poder Judiciário do Estado do Tocantins.

RESOLVE:

Art. 1º. Designar o servidor _____-, matrícula _____, como gestor do contrato nº ___/202__, e o servidor ____, matrícula _____, como seu substituto, para, nos termos do *"caput"* do artigo 67 da Lei nº. 8.666/93, conhecerem as obrigações mútuas previstas no instrumento de contratual, acompanhar e fiscalizar até a sua completa execução.

Parágrafo único – Verificada a ocorrência de falta ou defeito na execução do contrato, o gestor notificará a contratada para regularização do apontamento, caso em que, não sendo atendido ou justificado, no prazo estabelecido, deverá informar à autoridade competente sobre o ocorrido, para fins de aplicação das penalidades.

Art. 2º. Esta Portaria entra em vigor na data de sua publicação, revogando as disposições em contrário.

Publique-se.

Documento assinado eletronicamente por **Valdiney da Costa Vale, Assessor Jurídico**, em 28/06/2021, às 16:46, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Agno Paixão Saraiva, Servidor Cedido**, em 01/07/2021, às 13:03, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **3776143** e o código CRC **6589C751**.