PODER JUDICIÁRIO
ESTADO DO TOCANTINS

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

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 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$ 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**.