



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

Contrato Nº 128/2019 - PRESIDÊNCIA/DIGER/DIADM/DCC

PREGÃO ELETRÔNICO SRP Nº 56/2019
ATA DE REGISTRO DE PREÇOS Nº 139/2019
PROCESSO ORIGINÁRIO 19.0.000003897-3
PROCESSO 19.0.000031831-3

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 seu Diretor-Geral, o Senhor **JONAS DEMOSTENE RAMOS**, brasileiro, portador do RG nº. 2.257.484-1 - SSP/PR, inscrito no CPF/MF sob o nº. 455.662.839-34, residente e domiciliado nesta capital, doravante designado **CONTRATANTE** e, de 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, CEP - 59062-480, Natal/RN Telefone: (84) 4008-9454, *email: tecnologia@qualitek.com.br*, doravante designada **CONTRATADA**, neste ato representada por seu Sócio-Diretor Comercial, o 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 nº. 8.666/1993, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO:

1.1. O presente Instrumento tem por objeto a aquisição e renovação de licença de solução corporativa de Antivírus *Kaspersky Endpoint Security* incluindo atualizações e suporte técnico pelo período de 24 (vinte e quatro) meses, para atender as demandas do Poder Judiciário do Estado do Tocantins, conforme descrições e quantitativos abaixo:

ITEM	DESCRIÇÃO	QTDE.	UND.	VALOR UNITÁRIO	VALOR TOTAL
1	Renovação de licenças de solução corporativa de antivírus. Kaspersky Endpoint Security for Business SELECT, com vigência de 24 (vinte e quatro) meses.	700	Und.	R\$ 65,00	R\$ 45.500,00
2	Aquisição de licenças de solução corporativa de antivírus. Kaspersky Endpoint Security for Business SELECT, com vigência de 24 (vinte e quatro) meses.	150	Und.	R\$ 67,00	R\$ 10.050,00
Valor Total					R\$ 55.550,00

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 19.0.000003897-3 e 19.0.000031831-3 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 nº 56/2019, do CONTRATANTE; e

1.2.2. A Proposta de Preços e documentos que o acompanham, firmada pela CONTRATADA em 12 de setembro de 2019.

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 Eletrônico, conforme Edital e Processo Administrativo acima citados.

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

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

CLÁUSULA SEGUNDA – DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS:

2.1. Renovação de licenças de solução corporativa de antivírus:

2.1.1. Características Gerais:

2.1.1.1. Todas as licenças fornecidas terão validade de 24 (vinte e quatro) meses para atualizações inerentes ao produto;

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

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

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

2.1.2. Servidor de Administração e Console Administrativa:

2.1.2.1. Compatibilidade:

2.1.2.1.1. Microsoft Windows Server 2008 (Todas edições);

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

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

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

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

- 2.1.2.1.6. Microsoft Windows Server 2016 x64
- 2.1.2.1.7. Microsoft Windows Small Business Server 2008 (Todas edições);
- 2.1.2.1.8. Microsoft Windows Small Business Server 2011 (Todas edições);
- 2.1.2.1.9. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
- 2.1.2.1.10. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
- 2.1.2.1.11. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
- 2.1.2.1.12. Microsoft Windows 8 Professional / Enterprise x64;
- 2.1.2.1.13. Microsoft Windows 8.1 Professional / Enterprise x32;
- 2.1.2.1.14. Microsoft Windows 8.1 Professional / Enterprise x64;
- 2.1.2.1.15. Microsoft Windows 10 (Todas edições x32);
- 2.1.2.1.16. Microsoft Windows 10 (Todas edições x64);
- 2.1.2.2. Características:
 - 2.1.2.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
 - 2.1.2.2.2. Console deve ser baseada no modelo cliente/servidor;
 - 2.1.2.2.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
 - 2.1.2.2.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
 - 2.1.2.2.5. Deve permitir incluir usuários do AD para logarem na console de administração;
 - 2.1.2.2.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
 - 2.1.2.2.7. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
 - 2.1.2.2.8. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
 - 2.1.2.2.9. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
 - 2.1.2.2.10. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
 - 2.1.2.2.11. Deve armazenar histórico das alterações feitas em políticas;
 - 2.1.2.2.12. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
 - 2.1.2.2.13. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
 - 2.1.2.2.14. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
 - 2.1.2.2.15. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
 - 2.1.2.2.16. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
 - 2.1.2.2.17. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
 - 2.1.2.2.18. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
 - 2.1.2.2.19. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
 - 2.1.2.2.20. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
 - 2.1.2.2.21. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
 - 2.1.2.2.22. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
 - 2.1.2.2.23. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
 - 2.1.2.2.24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
 - 2.1.2.2.25. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
 - 2.1.2.2.26. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
 - 2.1.2.2.27. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
 - 2.1.2.2.28. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:
 - 2.1.2.2.28.1. Nome do computador;
 - 2.1.2.2.28.2. Nome do domínio;
 - 2.1.2.2.28.3. Range de IP;
 - 2.1.2.2.28.4. Sistema Operacional;
 - 2.1.2.2.28.5. Máquina virtual.
 - 2.1.2.2.29. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
 - 2.1.2.2.30. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
 - 2.1.2.2.31. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
 - 2.1.2.2.32. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

- 2.1.2.2.33. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
- 2.1.2.2.34. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;
- 2.1.2.2.35. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- 2.1.2.2.36. Deve fornecer as seguintes informações dos computadores:
- 2.1.2.2.36.1. Se o antivírus está instalado;
- 2.1.2.2.36.2. Se o antivírus está iniciado;
- 2.1.2.2.36.3. Se o antivírus está atualizado;
- 2.1.2.2.36.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
- 2.1.2.2.36.5. Minutos/horas desde a última atualização de vacinas;
- 2.1.2.2.36.6. Data e horário da última verificação executada na máquina;
- 2.1.2.2.36.7. Versão do antivírus instalado na máquina;
- 2.1.2.2.36.8. Se é necessário reiniciar o computador para aplicar mudanças;
- 2.1.2.2.36.9. Data e horário de quando a máquina foi ligada;
- 2.1.2.2.36.10. Quantidade de vírus encontrados (contador) na máquina;
- 2.1.2.2.36.11. Nome do computador;
- 2.1.2.2.36.12. Domínio ou grupo de trabalho do computador;
- 2.1.2.2.36.13. Data e horário da última atualização de vacinas;
- 2.1.2.2.36.14. Sistema operacional com Service Pack;
- 2.1.2.2.36.15. Quantidade de processadores;
- 2.1.2.2.36.16. Quantidade de memória RAM;
- 2.1.2.2.36.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
- 2.1.2.2.36.18. Endereço IP;
- 2.1.2.2.36.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
- 2.1.2.2.36.20. Atualizações do Windows Updates instaladas;
- 2.1.2.2.36.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
- 2.1.2.2.36.22. Vulnerabilidades de aplicativos instalados na máquina;
- 2.1.2.2.37. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- 2.1.2.2.38. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
- 2.1.2.2.38.1. Alteração de Gateway Padrão;
- 2.1.2.2.38.2. Alteração de subrede;
- 2.1.2.2.38.3. Alteração de domínio;
- 2.1.2.2.38.4. Alteração de servidor DHCP;
- 2.1.2.2.38.5. Alteração de servidor DNS;
- 2.1.2.2.38.6. Alteração de servidor WINS;
- 2.1.2.2.38.7. Alteração de subrede;
- 2.1.2.2.38.8. Resolução de Nome;
- 2.1.2.2.38.9. Disponibilidade de endereço de conexão SSL;
- 2.1.2.2.39. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 2.1.2.2.40. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- 2.1.2.2.41. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- 2.1.2.2.42. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 2.1.2.2.43. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
- 2.1.2.2.44. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
- 2.1.2.2.45. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
- 2.1.2.2.46. Capacidade de gerar traps SNMP para monitoramento de eventos;
- 2.1.2.2.47. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- 2.1.2.2.48. Listar em um único local, todos os computadores não gerenciados na rede;
- 2.1.2.2.49. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
- 2.1.2.2.50. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
- 2.1.2.2.51. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

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

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

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

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

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

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

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

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

2.1.2.2.59.1. Nome do vírus;

2.1.2.2.59.2. Nome do arquivo infectado;

2.1.2.2.59.3. Data e hora da detecção;

2.1.2.2.59.4. Nome da máquina ou endereço IP;

2.1.2.2.59.5. Ação realizada.

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

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

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

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

2.1.2.2.64. Capacidade de realizar resumo de hardware de cada máquina cliente;

2.1.2.2.65. Capacidade de realizar resumo de hardware de cada máquina cliente;

2.1.2.2.66. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2.1.3. Estações Windows

2.1.3.1. Compatibilidade:

2.1.3.1.1. Microsoft Windows XP Professional x86;

2.1.3.1.2. Microsoft Windows Vista x86 / x64 SP2;

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

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

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

2.1.3.1.6. Microsoft Windows 10 Pro / Enterprise x86 / x64;

2.1.3.1.7. Microsoft Windows Server 2012 R2 Standard x64;

2.1.3.1.8. Microsoft Windows Server 2012 Foundation x64;

2.1.3.1.9. Microsoft Windows Server 2012 Standard x64;

2.1.3.1.10. Microsoft Small Business Server 2011 Standard x64;

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

2.1.3.1.12. Microsoft Windows Server 2008 Standard/Enterprise x86/x64 SP2;

2.1.3.1.13. Microsoft Windows Server 2016 x64

2.1.3.2. Características:

2.1.3.2.1. Deve prover as seguintes proteções:

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

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

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

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

2.1.3.2.1.5. Firewall com IDS;

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

2.1.3.2.1.7. Controle de dispositivos externos;

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

2.1.3.2.1.9. Controle de acesso a sites por horário;

2.1.3.2.1.10. Controle de acesso a sites por usuários;

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

2.1.3.2.1.12. Controle de execução de aplicativos;

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

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

- 2.1.3.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
- 2.1.3.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 2.1.3.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 2.1.3.2.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
- 2.1.3.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 2.1.3.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 2.1.3.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 2.1.3.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
- 2.1.3.2.11. Capacidade de verificar somente arquivos novos e alterados;
- 2.1.3.2.12. Capacidade de verificar objetos usando heurística;
- 2.1.3.2.13. Capacidade de agendar uma pausa na verificação;
- 2.1.3.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
- 2.1.3.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 2.1.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- 2.1.3.2.16.1. Perguntar o que fazer, ou;
- 2.1.3.2.16.2. Bloquear acesso ao objeto;
- 2.1.3.2.16.3. Apagar o objeto ou tentar desinfecção-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.1.3.2.16.3.1. Caso positivo de desinfecção:
- 2.1.3.2.16.3.1.1. Restaurar o objeto para uso;
- 2.1.3.2.16.3.2. Caso negativo de desinfecção:
- 2.1.3.2.16.3.2.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.1.3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 2.1.3.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;
- 2.1.3.2.19. Capacidade de verificar links inseridos em e-mails contra phishings;
- 2.1.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
- 2.1.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- 2.1.3.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
- 2.1.3.2.22.1. Perguntar o que fazer, ou;
- 2.1.3.2.22.2. Bloquear o e-mail;
- 2.1.3.2.22.3. Apagar o objeto ou tentar desinfecção-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.1.3.2.22.3.1. Caso positivo de desinfecção:
- 2.1.3.2.22.3.1.1. Restaurar o e-mail para o usuário;
- 2.1.3.2.22.3.2. Caso negativo de desinfecção:
- 2.1.3.2.22.3.2.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.1.3.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
- 2.1.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
- 2.1.3.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
- 2.1.3.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
- 2.1.3.2.27. Deve ter suporte total ao protocolo Ipv6;
- 2.1.3.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
- 2.1.3.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
- 2.1.3.2.29.1. Perguntar o que fazer, ou;
- 2.1.3.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
- 2.1.3.2.29.3. Permitir acesso ao objeto;
- 2.1.3.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
- 2.1.3.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
- 2.1.3.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
- 2.1.3.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
- 2.1.3.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
- 2.1.3.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

- 2.1.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;
- 2.1.3.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (<http://www.antiphishing.org/>);
- 2.1.3.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
- 2.1.3.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;
- 2.1.3.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
- 2.1.3.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
- 2.1.3.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 2.1.3.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
- 2.1.3.2.39.1. Discos de armazenamento locais;
- 2.1.3.2.39.2. Armazenamento removível;
- 2.1.3.2.39.3. Impressoras;
- 2.1.3.2.39.4. CD/DVD;
- 2.1.3.2.39.5. Drives de disquete;
- 2.1.3.2.39.6. Modems;
- 2.1.3.2.39.7. Dispositivos de fita;
- 2.1.3.2.39.8. Dispositivos multifuncionais;
- 2.1.3.2.39.9. Leitores de smart card;
- 2.1.3.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
- 2.1.3.2.39.11. Wi-Fi;
- 2.1.3.2.39.12. Adaptadores de rede externos;
- 2.1.3.2.39.13. Dispositivos MP3 ou smartphones;
- 2.1.3.2.39.14. Dispositivos Bluetooth;
- 2.1.3.2.39.15. Câmeras e Scanners.
- 2.1.3.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
- 2.1.3.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
- 2.1.3.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
- 2.1.3.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos, etc.
- 2.1.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
- 2.1.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);
- 2.1.3.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:
- 2.1.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
- 2.1.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
- 2.1.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
- 2.1.3.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
- 2.1.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
- 2.1.3.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
- 2.1.3.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.
- 2.1.3.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
- 2.1.3.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
- 2.1.3.2.54. Capacidade de integração com o Windows Defender Security Center.
- 2.1.3.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).
- 2.1.3.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).
- 2.1.4. Estações Mac OS X
- 2.1.4.1. Compatibilidade:
- 2.1.4.1.1. macOS High Sierra 10.13
- 2.1.4.1.2. macOS Sierra 10.12
- 2.1.4.1.3. Mac OS X 10.11 (El Capitan);
- 2.1.4.1.4. Mac OS X 10.10 (Yosemite);
- 2.1.4.1.5. Mac OS X 10.9 (Mavericks);

2.1.4.2. Características:

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

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

2.1.4.2.3. Possuir módulo de bloqueio á ataques na rede;

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

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

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

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

2.1.4.2.8. Deve possuir suportes a notificações utilizando o Growl;

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

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

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

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

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

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

2.1.4.2.15. Capacidade de verificar somente arquivos novos e alterados;

2.1.4.2.16. Capacidade de verificar objetos usando heurística;

2.1.4.2.17. Capacidade de agendar uma pausa na verificação;

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

2.1.4.2.18.1. Perguntar o que fazer, ou;

2.1.4.2.18.2. Bloquear acesso ao objeto;

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

2.1.4.2.18.4. Caso positivo de desinfecção:

2.1.4.2.18.4.1. Restaurar o objeto para uso;

2.1.4.2.18.5. Caso negativo de desinfecção:

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

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

2.1.4.2.20. Capacidade de verificar arquivos de formato de email;

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

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

2.1.5. Estações Linux

2.1.5.1. Compatibilidade:

2.1.5.1.1. Plataforma 32 ou 64 bits:

2.1.5.1.1.1. Red Hat 5.x ou superior;

2.1.5.1.1.2. CentOS 6 ou superior;

2.1.5.1.1.3. Ubuntu 12.04 LTS ou superior;

2.1.5.2. Características

2.1.5.2.1. Deve prover as seguintes proteções:

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

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

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

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

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

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

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

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

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

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

- 2.1.5.2.6. Capacidade de verificar objetos usando heurística;
- 2.1.5.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- 2.1.5.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- 2.1.5.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
- 2.1.6. Servidores Windows
 - 2.1.6.1. Compatibilidade:
 - 2.1.6.1.1. Microsoft Windows Server 2008 ou superior;
 - 2.1.6.1.2. Microsoft Windows Hyper-V Server 2008 ou superior;
 - 2.1.6.2. Características:
 - 2.1.6.2.1. Deve prover as seguintes proteções:
 - 2.1.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 2.1.6.2.1.2. Autoproteção contra ataques aos serviços/processos do antivírus;
 - 2.1.6.2.1.3. Firewall com IDS;
 - 2.1.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.
 - 2.1.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
 - 2.1.6.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
 - 2.1.6.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 2.1.6.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 2.1.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
 - 2.1.6.2.4.3. Leitura de configurações;
 - 2.1.6.2.4.4. Modificação de configurações;
 - 2.1.6.2.4.5. Gerenciamento de Backup e Quarentena;
 - 2.1.6.2.4.6. Visualização de relatórios;
 - 2.1.6.2.4.7. Gerenciamento de relatórios;
 - 2.1.6.2.4.8. Gerenciamento de chaves de licença;
 - 2.1.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).
 - 2.1.6.2.5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
 - 2.1.6.2.5.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
 - 2.1.6.2.5.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
 - 2.1.6.2.6. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.
 - 2.1.6.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc)
 - 2.1.6.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS)
 - 2.1.6.2.9. Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
 - 2.1.6.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.
 - 2.1.6.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.
 - 2.1.6.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.
 - 2.1.6.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
 - 2.1.6.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
 - 2.1.6.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
 - 2.1.6.2.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
 - 2.1.6.2.17. Capacidade de verificar somente arquivos novos e alterados;
 - 2.1.6.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto-descompressores, .PST, arquivos compactados por compactadores binários, etc);
 - 2.1.6.2.19. Capacidade de verificar objetos usando heurística;
 - 2.1.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
 - 2.1.6.2.21. Capacidade de agendar uma pausa na verificação;
 - 2.1.6.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
 - 2.1.6.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.1.6.2.23.1. Perguntar o que fazer, ou;
 - 2.1.6.2.23.2. Bloquear acesso ao objeto;
 - 2.1.6.2.23.2.1. Apagar o objeto ou tentar desinfecá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

- 2.1.6.2.23.2.2. Caso positivo de desinfecção:
 - 2.1.6.2.23.2.2.1. Restaurar o objeto para uso;
 - 2.1.6.2.23.2.3. Caso negativo de desinfecção:
 - 2.1.6.2.23.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).
 - 2.1.6.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
 - 2.1.6.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
 - 2.1.6.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
 - 2.1.6.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
 - 2.1.6.2.28. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;
 - 2.1.6.2.29. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning);
 - 2.1.6.2.30. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.
- 2.1.7. Servidores Linux
 - 2.1.7.1. Compatibilidade:
 - 2.1.7.1.1. Plataforma 32 e 64 bits:
 - 2.1.7.1.1.1. Red Hat 5.x ou superior;
 - 2.1.7.1.1.2. CentOS 6 ou superior;
 - 2.1.7.1.1.3. Ubuntu 12.04 LTS ou superior;
 - 2.1.7.2. Características:
 - 2.1.7.2.1. Deve prover as seguintes proteções:
 - 2.1.7.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 2.1.7.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
 - 2.1.7.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 2.1.7.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 2.1.7.2.2.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
 - 2.1.7.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
 - 2.1.7.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
 - 2.1.7.2.3. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
 - 2.1.7.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
 - 2.1.7.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
 - 2.1.7.2.6. Capacidade de verificar objetos usando heurística;
 - 2.1.7.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
 - 2.1.7.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
 - 2.1.7.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
 - 2.1.8. Smartphones e tablets
 - 2.1.8.1. Compatibilidade:
 - 2.1.8.1.1. Android 7.0 – 7.12
 - 2.1.8.1.2. Android 8.0 – 8.1
 - 2.1.8.1.3. iOS 9.0 – 9.3.5
 - 2.1.8.1.4. iOS 10.0 – 10.3.3
 - 2.1.8.1.5. iOS 11.0 – 11.3
 - 2.1.8.2. Características:
 - 2.1.8.2.1. Deve prover as seguintes proteções:
 - 2.1.8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
 - 2.1.8.2.1.1.1. Todos os objetos transmitidos usando conexões wireless (porta de infra-vermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.
 - 2.1.8.2.1.1.2. Arquivos abertos no smartphone
 - 2.1.8.2.1.1.3. Programas instalados usando a interface do smartphone
 - 2.1.8.2.1.2. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
 - 2.1.8.2.2. Deverá isolar em área de quarentena os arquivos infectados;
 - 2.1.8.2.3. Deverá atualizar as bases de vacinas de modo agendado;
 - 2.1.8.2.4. Deverá bloquear spams de SMS através de Black lists;

- 2.1.8.2.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;
- 2.1.8.2.6. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
- 2.1.8.2.7. Deverá ter firewall pessoal;
- 2.1.8.2.8. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Devive Manager 2008 SP1;
- 2.1.8.2.9. Possibilidade de instalação remota utilizando o Sybase Afaia 6.5;
- 2.1.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS;
- 2.1.8.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos;
- 2.1.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso;
- 2.1.8.2.13. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
- 2.1.8.2.14. Capacidade de configurar White e black list de aplicativos.
- 2.1.9. Gerenciamento de dispositivos móveis (MDM):
 - 2.1.9.1. Compatibilidade:
 - 2.1.9.1.1. Android 5.0 – 5.1.1
 - 2.1.9.1.2. Android 6.0 – 6.0.1
 - 2.1.9.1.3. Android 7.0 – 7.12
 - 2.1.9.1.4. Android 8.0 – 8.1
 - 2.1.9.1.5. iOS 9.0 – 9.3.5
 - 2.1.9.1.6. iOS 10.0 – 10.3.3
 - 2.1.9.1.7. iOS 11.0 – 11.3
 - 2.1.9.2. Características:
 - 2.1.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
 - 2.1.9.2.2. Capacidade de ajustar as configurações de:
 - 2.1.9.2.2.1. Sincronização de e-mail;
 - 2.1.9.2.2.2. Uso de aplicativos;
 - 2.1.9.2.2.3. Senha do usuário;
 - 2.1.9.2.2.4. Criptografia de dados;
 - 2.1.9.2.2.5. Conexão de mídia removível.
 - 2.1.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
 - 2.1.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS;
 - 2.1.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
 - 2.1.9.3. Capacidade de, remotamente, bloquear um dispositivo iOS.

2.2. Aquisição de licenças de solução corporativa de antivírus

- 2.2.1. Características Gerais:
 - 2.2.1.1. Todas as licenças fornecidas terão validade de 24 (vinte e quatro) meses para atualizações inerentes ao produto;
 - 2.2.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus quanto do software;
 - 2.2.1.3. As atualizações deverão ser disponibilizadas através de site na Internet ou através do próprio software;
 - 2.2.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para o Contratante além daquele já cotado na proposta.
- 2.2.2. Servidor de Administração e Console Administrativa
 - 2.2.2.1. Compatibilidade:
 - 2.2.2.1.1. Microsoft Windows Server 2008 (Todas edições);
 - 2.2.2.1.2. Microsoft Windows Server 2008 x64 SP1 (Todas edições);
 - 2.2.2.1.3. Microsoft Windows Server 2008 R2 (Todas edições);
 - 2.2.2.1.4. Microsoft Windows Server 2012 (Todas edições x64);
 - 2.2.2.1.5. Microsoft Windows Server 2012 R2 (Todas edições x64);
 - 2.2.2.1.6. Microsoft Windows Server 2016 x64
 - 2.2.2.1.7. Microsoft Windows Small Business Server 2008 (Todas edições);
 - 2.2.2.1.8. Microsoft Windows Small Business Server 2011 (Todas edições);
 - 2.2.2.1.9. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
 - 2.2.2.1.10. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
 - 2.2.2.1.11. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
 - 2.2.2.1.12. Microsoft Windows 8 Professional / Enterprise x64;
 - 2.2.2.1.13. Microsoft Windows 8.1 Professional / Enterprise x32;
 - 2.2.2.1.14. Microsoft Windows 8.1 Professional / Enterprise x64;
 - 2.2.2.1.15. Microsoft Windows 10 (Todas edições x32);
 - 2.2.2.1.16. Microsoft Windows 10 (Todas edições x64);
 - 2.2.2.2. Características:

- 2.2.2.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
- 2.2.2.2.2. Console deve ser baseada no modelo cliente/servidor;
- 2.2.2.2.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
- 2.2.2.2.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
- 2.2.2.2.5. Deve permitir incluir usuários do AD para logarem na console de administração;
- 2.2.2.2.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
- 2.2.2.2.7. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
- 2.2.2.2.8. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
- 2.2.2.2.9. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
- 2.2.2.2.10. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
- 2.2.2.2.11. Deve armazenar histórico das alterações feitas em políticas;
- 2.2.2.2.12. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
- 2.2.2.2.13. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
- 2.2.2.2.14. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
- 2.2.2.2.15. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
- 2.2.2.2.16. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
- 2.2.2.2.17. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
- 2.2.2.2.18. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
- 2.2.2.2.19. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
- 2.2.2.2.20. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
- 2.2.2.2.21. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
- 2.2.2.2.22. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
- 2.2.2.2.23. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- 2.2.2.2.24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- 2.2.2.2.25. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
- 2.2.2.2.26. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
- 2.2.2.2.27. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
- 2.2.2.2.28. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:
 - 2.2.2.2.28.1. Nome do computador;
 - 2.2.2.2.28.2. Nome do domínio;
 - 2.2.2.2.28.3. Range de IP;
 - 2.2.2.2.28.4. Sistema Operacional;
 - 2.2.2.2.28.5. Máquina virtual.
- 2.2.2.2.29. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
- 2.2.2.2.30. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
- 2.2.2.2.31. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
- 2.2.2.2.32. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
- 2.2.2.2.33. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
- 2.2.2.2.34. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;
- 2.2.2.2.35. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- 2.2.2.2.36. Deve fornecer as seguintes informações dos computadores:
 - 2.2.2.2.36.1. Se o antivírus está instalado;
 - 2.2.2.2.36.2. Se o antivírus está iniciado;
 - 2.2.2.2.36.3. Se o antivírus está atualizado;
 - 2.2.2.2.36.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
 - 2.2.2.2.36.5. Minutos/horas desde a última atualização de vacinas;
 - 2.2.2.2.36.6. Data e horário da última verificação executada na máquina;

- 2.2.2.2.36.7. Versão do antivírus instalado na máquina;
- 2.2.2.2.36.8. Se é necessário reiniciar o computador para aplicar mudanças;
- 2.2.2.2.36.9. Data e horário de quando a máquina foi ligada;
- 2.2.2.2.36.10. Quantidade de vírus encontrados (contador) na máquina;
- 2.2.2.2.36.11. Nome do computador;
- 2.2.2.2.36.12. Domínio ou grupo de trabalho do computador;
- 2.2.2.2.36.13. Data e horário da última atualização de vacinas;
- 2.2.2.2.36.14. Sistema operacional com Service Pack;
- 2.2.2.2.36.15. Quantidade de processadores;
- 2.2.2.2.36.16. Quantidade de memória RAM;
- 2.2.2.2.36.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
- 2.2.2.2.36.18. Endereço IP;
- 2.2.2.2.36.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
- 2.2.2.2.36.20. Atualizações do Windows Updates instaladas;
- 2.2.2.2.36.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
- 2.2.2.2.36.22. Vulnerabilidades de aplicativos instalados na máquina;
- 2.2.2.2.37. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- 2.2.2.2.38. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
 - 2.2.2.2.38.1. Alteração de Gateway Padrão;
 - 2.2.2.2.38.2. Alteração de subrede;
 - 2.2.2.2.38.3. Alteração de domínio;
 - 2.2.2.2.38.4. Alteração de servidor DHCP;
 - 2.2.2.2.38.5. Alteração de servidor DNS;
 - 2.2.2.2.38.6. Alteração de servidor WINS;
 - 2.2.2.2.38.7. Alteração de subrede;
 - 2.2.2.2.38.8. Resolução de Nome;
 - 2.2.2.2.38.9. Disponibilidade de endereço de conexão SSL;
- 2.2.2.2.39. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 2.2.2.2.40. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- 2.2.2.2.41. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- 2.2.2.2.42. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 2.2.2.2.43. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
- 2.2.2.2.44. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
- 2.2.2.2.45. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
- 2.2.2.2.46. Capacidade de gerar traps SNMP para monitoramento de eventos;
- 2.2.2.2.47. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- 2.2.2.2.48. Listar em um único local, todos os computadores não gerenciados na rede;
- 2.2.2.2.49. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
- 2.2.2.2.50. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
- 2.2.2.2.51. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;
- 2.2.2.2.52. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
- 2.2.2.2.53. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
- 2.2.2.2.54. Deve através de opções de otimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;
- 2.2.2.2.55. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);
- 2.2.2.2.56. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;
- 2.2.2.2.57. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;
- 2.2.2.2.58. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
- 2.2.2.2.59. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

- 2.2.2.2.59.1. Nome do vírus;
- 2.2.2.2.59.2. Nome do arquivo infectado;
- 2.2.2.2.59.3. Data e hora da detecção;
- 2.2.2.2.59.4. Nome da máquina ou endereço IP;
- 2.2.2.2.59.5. Ação realizada.
- 2.2.2.2.60. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
- 2.2.2.2.61. Capacidade de listar updates nas máquinas com o respectivo link para download
- 2.2.2.2.62. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;
- 2.2.2.2.63. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
- 2.2.2.2.64. Capacidade de realizar resumo de hardware de cada máquina cliente;
- 2.2.2.2.65. Capacidade de realizar resumo de hardware de cada máquina cliente;
- 2.2.2.2.66. Capacidade de diferenciar máquinas virtuais de máquinas físicas.
- 2.2.3. Estações Windows
 - 2.2.3.1. Compatibilidade:
 - 2.2.3.1.1. Microsoft Windows XP Professional x86;
 - 2.2.3.1.2. Microsoft Windows Vista x86 / x64 SP2;
 - 2.2.3.1.3. Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
 - 2.2.3.1.4. Microsoft Windows 8 Professional/Enterprise x86 / x64;
 - 2.2.3.1.5. Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
 - 2.2.3.1.6. Microsoft Windows 10 Pro / Enterprise x86 / x64;
 - 2.2.3.1.7. Microsoft Windows Server 2012 R2 Standard x64;
 - 2.2.3.1.8. Microsoft Windows Server 2012 Foundation x64;
 - 2.2.3.1.9. Microsoft Windows Server 2012 Standard x64;
 - 2.2.3.1.10. Microsoft Small Business Server 2011 Standard x64;
 - 2.2.3.1.11. Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1;
 - 2.2.3.1.12. Microsoft Windows Server 2008 Standard/Enterprise x86/x64 SP2;
 - 2.2.3.1.13. Microsoft Windows Server 2016 x64
 - 2.2.3.2. Características:
 - 2.2.3.2.1. Deve prover as seguintes proteções:
 - 2.2.3.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 2.2.3.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
 - 2.2.3.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
 - 2.2.3.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
 - 2.2.3.2.1.5. Firewall com IDS;
 - 2.2.3.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);
 - 2.2.3.2.1.7. Controle de dispositivos externos;
 - 2.2.3.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
 - 2.2.3.2.1.9. Controle de acesso a sites por horário;
 - 2.2.3.2.1.10. Controle de acesso a sites por usuários;
 - 2.2.3.2.1.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
 - 2.2.3.2.1.12. Controle de execução de aplicativos;
 - 2.2.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
 - 2.2.3.2.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
 - 2.2.3.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
 - 2.2.3.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
 - 2.2.3.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
 - 2.2.3.2.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
 - 2.2.3.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
 - 2.2.3.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
 - 2.2.3.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

- 2.2.3.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
- 2.2.3.2.11. Capacidade de verificar somente arquivos novos e alterados;
- 2.2.3.2.12. Capacidade de verificar objetos usando heurística;
- 2.2.3.2.13. Capacidade de agendar uma pausa na verificação;
- 2.2.3.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
- 2.2.3.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 2.2.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.2.3.2.16.1. Perguntar o que fazer, ou;
 - 2.2.3.2.16.2. Bloquear acesso ao objeto;
 - 2.2.3.2.16.3. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.3.2.16.3.1. Caso positivo de desinfecção:
 - 2.2.3.2.16.3.1.1. Restaurar o objeto para uso;
 - 2.2.3.2.16.3.2. Caso negativo de desinfecção:
 - 2.2.3.2.16.3.2.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
 - 2.2.3.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;
 - 2.2.3.2.19. Capacidade de verificar links inseridos em e-mails contra phishings;
 - 2.2.3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
 - 2.2.3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
 - 2.2.3.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.2.3.2.22.1. Perguntar o que fazer, ou;
 - 2.2.3.2.22.2. Bloquear o e-mail;
 - 2.2.3.2.22.3. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.3.2.22.3.1. Caso positivo de desinfecção:
 - 2.2.3.2.22.3.1.1. Restaurar o e-mail para o usuário;
 - 2.2.3.2.22.3.2. Caso negativo de desinfecção:
 - 2.2.3.2.22.3.2.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.3.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
 - 2.2.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
 - 2.2.3.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
 - 2.2.3.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
 - 2.2.3.2.27. Deve ter suporte total ao protocolo Ipv6;
 - 2.2.3.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
 - 2.2.3.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
 - 2.2.3.2.29.1. Perguntar o que fazer, ou;
 - 2.2.3.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
 - 2.2.3.2.29.3. Permitir acesso ao objeto;
 - 2.2.3.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
 - 2.2.3.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
 - 2.2.3.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
 - 2.2.3.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
 - 2.2.3.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
 - 2.2.3.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
 - 2.2.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;
 - 2.2.3.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (<http://www.antiphishing.org/>);
 - 2.2.3.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
 - 2.2.3.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;
 - 2.2.3.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
 - 2.2.3.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
 - 2.2.3.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
 - 2.2.3.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
 - 2.2.3.2.39.1. Discos de armazenamento locais;

- 2.2.3.2.39.2. Armazenamento removível;
- 2.2.3.2.39.3. Impressoras;
- 2.2.3.2.39.4. CD/DVD;
- 2.2.3.2.39.5. Drives de disquete;
- 2.2.3.2.39.6. Modems;
- 2.2.3.2.39.7. Dispositivos de fita;
- 2.2.3.2.39.8. Dispositivos multifuncionais;
- 2.2.3.2.39.9. Leitores de smart card;
- 2.2.3.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
- 2.2.3.2.39.11. Wi-Fi;
- 2.2.3.2.39.12. Adaptadores de rede externos;
- 2.2.3.2.39.13. Dispositivos MP3 ou smartphones;
- 2.2.3.2.39.14. Dispositivos Bluetooth;
- 2.2.3.2.39.15. Câmeras e Scanners.
- 2.2.3.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
- 2.2.3.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
- 2.2.3.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
- 2.2.3.2.43. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.
- 2.2.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
- 2.2.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);
- 2.2.3.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:
 - 2.2.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
 - 2.2.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
- 2.2.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
- 2.2.3.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
- 2.2.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
- 2.2.3.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
- 2.2.3.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.
- 2.2.3.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
- 2.2.3.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
- 2.2.3.2.54. Capacidade de integração com o Windows Defender Security Center.
- 2.2.3.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).
- 2.2.3.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).
- 2.2.4. Estações Mac OS X
 - 2.2.4.1. Compatibilidade:
 - 2.2.4.1.1. macOS High Sierra 10.13
 - 2.2.4.1.2. macOS Sierra 10.12
 - 2.2.4.1.3. Mac OS X 10.11 (El Capitan);
 - 2.2.4.1.4. Mac OS X 10.10 (Yosemite);
 - 2.2.4.1.5. Mac OS X 10.9 (Mavericks);
 - 2.2.4.2. Características:
 - 2.2.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 2.2.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https;
 - 2.2.4.2.3. Possuir módulo de bloqueio á ataques na rede;
 - 2.2.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
 - 2.2.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio á ataques na rede;
 - 2.2.4.2.6. Possibilidade de importar uma chave no pacote de instalação;
 - 2.2.4.2.7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
 - 2.2.4.2.8. Deve possuir suportes a notificações utilizando o Growl;
 - 2.2.4.2.9. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
 - 2.2.4.2.10. Capacidade de voltar para a base de dados de vacina anterior;

- 2.2.4.2.11. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
- 2.2.4.2.12. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 2.2.4.2.13. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 2.2.4.2.14. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 2.2.4.2.15. Capacidade de verificar somente arquivos novos e alterados;
- 2.2.4.2.16. Capacidade de verificar objetos usando heurística;
- 2.2.4.2.17. Capacidade de agendar uma pausa na verificação;
- 2.2.4.2.18. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.2.4.2.18.1. Perguntar o que fazer, ou;
 - 2.2.4.2.18.2. Bloquear acesso ao objeto;
 - 2.2.4.2.18.3. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.4.2.18.4. Caso positivo de desinfecção:
 - 2.2.4.2.18.4.1. Restaurar o objeto para uso;
 - 2.2.4.2.18.5. Caso negativo de desinfecção:
 - 2.2.4.2.18.5.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.4.2.19. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
 - 2.2.4.2.20. Capacidade de verificar arquivos de formato de email;
 - 2.2.4.2.21. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
 - 2.2.4.2.22. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.
- 2.2.5. Estações Linux
 - 2.2.5.1. Compatibilidade:
 - 2.2.5.1.1. Plataforma 32 ou 64 bits:
 - 2.2.5.1.1.1. Red Hat 5.x ou superior;
 - 2.2.5.1.1.2. CentOS 6 ou superior;
 - 2.2.5.1.1.3. Ubuntu 12.04 LTS ou superior;
 - 2.2.5.2. Características
 - 2.2.5.2.1. Deve prover as seguintes proteções:
 - 2.2.5.2.1.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 2.2.5.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
 - 2.2.5.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 2.2.5.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 2.2.5.2.2.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfecção e remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
 - 2.2.5.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
 - 2.2.5.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
 - 2.2.5.2.3. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
 - 2.2.5.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
 - 2.2.5.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
 - 2.2.5.2.6. Capacidade de verificar objetos usando heurística;
 - 2.2.5.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
 - 2.2.5.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
 - 2.2.5.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
 - 2.2.6. Servidores Windows
 - 2.2.6.1. Compatibilidade:
 - 2.2.6.1.1. Microsoft Windows Server 2008 ou superior;
 - 2.2.6.1.2. Microsoft Windows Hyper-V Server 2008 ou superior;
 - 2.2.6.2. Características:
 - 2.2.6.2.1. Deve prover as seguintes proteções:
 - 2.2.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 2.2.6.2.1.2. Autoproteção contra ataques aos serviços/processos do antivírus;

- 2.2.6.2.1.3. Firewall com IDS;
- 2.2.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.
- 2.2.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 2.2.6.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
- 2.2.6.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 2.2.6.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 2.2.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
 - 2.2.6.2.4.3. Leitura de configurações;
 - 2.2.6.2.4.4. Modificação de configurações;
 - 2.2.6.2.4.5. Gerenciamento de Backup e Quarentena;
 - 2.2.6.2.4.6. Visualização de relatórios;
 - 2.2.6.2.4.7. Gerenciamento de relatórios;
 - 2.2.6.2.4.8. Gerenciamento de chaves de licença;
 - 2.2.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).
- 2.2.6.2.5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
 - 2.2.6.2.5.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
 - 2.2.6.2.5.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 2.2.6.2.6. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.
- 2.2.6.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc)
- 2.2.6.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS)
- 2.2.6.2.9. Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
- 2.2.6.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.
- 2.2.6.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.
- 2.2.6.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.
- 2.2.6.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 2.2.6.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 2.2.6.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 2.2.6.2.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
- 2.2.6.2.17. Capacidade de verificar somente arquivos novos e alterados;
- 2.2.6.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto-descompressores, .PST, arquivos compactados por compactadores binários, etc);
- 2.2.6.2.19. Capacidade de verificar objetos usando heurística;
- 2.2.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- 2.2.6.2.21. Capacidade de agendar uma pausa na verificação;
- 2.2.6.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 2.2.6.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.2.6.2.23.1. Perguntar o que fazer, ou;
 - 2.2.6.2.23.2. Bloquear acesso ao objeto;
 - 2.2.6.2.23.2.1. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.6.2.23.2.2. Caso positivo de desinfecção:
 - 2.2.6.2.23.2.2.1. Restaurar o objeto para uso;
 - 2.2.6.2.23.2.3. Caso negativo de desinfecção:
 - 2.2.6.2.23.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).
- 2.2.6.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 2.2.6.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- 2.2.6.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- 2.2.6.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
- 2.2.6.2.28. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;
- 2.2.6.2.29. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning);
- 2.2.6.2.30. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

2.2.7. Servidores Linux

2.2.7.1. Compatibilidade:

2.2.7.1.1. Plataforma 32 e 64 bits:

2.2.7.1.1.1. Red Hat 5.x ou superior;

2.2.7.1.1.2. CentOS 6 ou superior;

2.2.7.1.1.3. Ubuntu 12.04 LTS ou superior;

2.2.7.2. Características:

2.2.7.2.1. Deve prover as seguintes proteções:

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

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

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

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

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

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

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

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

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

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

2.2.7.2.6. Capacidade de verificar objetos usando heurística;

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

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

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

2.2.8. Smartphones e tablets

2.2.8.1. Compatibilidade:

2.2.8.1.1. Android 7.0 – 7.12

2.2.8.1.2. Android 8.0 – 8.1

2.2.8.1.3. iOS 9.0 – 9.3.5

2.2.8.1.4. iOS 10.0 – 10.3.3

2.2.8.1.5. iOS 11.0 – 11.3

2.2.8.2. Características:

2.2.8.2.1. Deve prover as seguintes proteções:

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

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

2.2.8.2.1.1.2. Arquivos abertos no smartphone

2.2.8.2.1.1.3. Programas instalados usando a interface do smartphone

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

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

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

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

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

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

2.2.8.2.7. Deverá ter firewall pessoal;

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

2.2.8.2.9. Possibilidade de instalação remota utilizando o Sybase Afaria 6.5;

2.2.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS;

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

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

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

2.2.8.2.14. Capacidade de configurar White e black list de aplicativos.

2.2.9. Gerenciamento de dispositivos móveis (MDM):

2.2.9.1. Compatibilidade:

2.2.9.1.1. Android 5.0 – 5.1.1

2.2.9.1.2. Android 6.0 – 6.0.1

2.2.9.1.3. Android 7.0 – 7.12

2.2.9.1.4. Android 8.0 – 8.1

2.2.9.1.5. iOS 9.0 – 9.3.5

2.2.9.1.6. iOS 10.0 – 10.3.3

2.2.9.1.7. iOS 11.0 – 11.3

2.2.9.2. Características:

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

2.2.9.2.2. Capacidade de ajustar as configurações de:

2.2.9.2.2.1. Sincronização de e-mail;

2.2.9.2.2.2. Uso de aplicativos;

2.2.9.2.2.3. Senha do usuário;

2.2.9.2.2.4. Criptografia de dados;

2.2.9.2.2.5. Conexão de mídia removível.

2.2.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;

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

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

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

2.3. Transferência de conhecimento e direitos de propriedade intelectual:

2.3.1. O uso de uma solução de antivírus corporativo é imprescindível por conter funções de proteção que vão além de um antivírus comum, evitando, portanto, invasões ou roubos de informações, por exemplo. Por isso, não existe versões corporativas gratuitas, não sendo vislumbrada outra forma de utilização senão a obrigatoriedade da aquisição dessa tecnologia de terceiros.

2.3.2. Os antivírus corporativos são produtos consolidados no mercado de Tecnologia da Informação e Comunicação no Brasil e utilizados por organizações públicas e privadas. Desta forma, os riscos de descontinuidade desse produto no mercado parece ser mínimo.

2.3.3. A CONTRATADA deverá realizar a transferência de conhecimento nas versões dos softwares que serão adquiridos pelo Contratante e com isso, repassar informações de configuração, testes, procedimentos de contingência e demais informações necessárias para a operação e manutenção da solução.

2.3.4. Quanto aos direitos de propriedade intelectual, não se aplica ao contexto desta contratação, uma vez que não será produzido nenhum artefato, tampouco trata de desenvolvimento de software.

CLÁUSULA TERCEIRA – DA DINÂMICA DE EXECUÇÃO

3.1. 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, quando não houver outro referido na coluna “Quando ocorre”.

ETAPA	DESCRIÇÃO	QUANDO OCORRE
1	Recebimento do pedido de fornecimento.	O Tribunal de Justiça encaminhará o pedido de fornecimento a qualquer tempo dentro da vigência da Ata de Registro de Preços e após a emissão da nota de empenho.
2	Entrega das licenças.	O prazo será de até 30 (trinta) dias subsequentes, contados a partir da data de envio 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, II, “a”, 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, 10 (dez) dias úteis, contados do primeiro dia útil posterior à entrega dos equipamentos, o Termo de Recebimento Definitivo, nos termos do artigo 73, II, “b”, 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 24 (vinte e quatro) meses.

CLÁUSULA QUARTA– DO LOCAL DE ENTREGA:

4.1. Os softwares bem como suas licenças deverão ser entregues na Diretoria de Tecnologia da Informação do Tribunal de Justiça do Estado do Tocantins, localizada no Anexo I do Tribunal de Justiça do Estado do Tocantins, situado na Quadra 103 Norte, Rua NO 11, Lote 2, 3º Andar, Plano Diretor Norte, Palmas/TO, CEP 77.001-036.

CLÁUSULA QUINTA – DO RECEBIMENTO:

5.1. O CONTRATANTE expedirá “Termo de Recebimento Provisório”, o qual deverá ser assinado pelo gestor deste Contrato, para efeito de posterior verificação da conformidade dos objetos, licenças, com as especificações constantes neste Instrumento e no Termo de Referência, nos termos do artigo 73, I, “a”, da Lei nº 8.666, de 1993.

5.2. Após a verificação da qualidade e quantidade dos objetos, licenças, e consequente aceitação, nos termos do artigo 73, I, “b”, da Lei nº 8.666, 1993, o CONTRATANTE emitirá “Termo de Recebimento Definitivo”, no prazo de 15 (quinze) dias, o qual deverá ser assinado pelo gestor.

5.3. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança dos bens fornecidos, nem ético-profissional, para perfeita execução do objeto, dentro dos limites estabelecidos pela lei ou pelo contrato.

5.4. A CONTRATADA é obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

CLÁUSULA SEXTA – DA GARANTIA E SUPORTE:

6.1. Garantia:

6.1.1. Durante o período de vigência do contrato a garantia se dará em forma de suporte técnico e seguirá especificações descritas neste Instrumento e no Termo de Referência que tratarão as respostas a incidentes de segurança;

6.1.2. O período de garantia será de 24 (vinte e quatro) meses, contados a partir da data do recebimento definitivo das licenças.

6.1.3. A localização para efeitos de garantia/suporte técnico deverá considerar o seguinte endereço: Palácio da Justiça Rio Tocantins, Praça dos Girassóis s/n, Palmas-TO, CEP 77.001-002;

6.1.4. Incluem-se, na garantia, os serviços de manutenção, suporte técnico, atualização de software e produto, bem como outras despesas decorrentes destes serviços, sem ônus ao CONTRATANTE, salvo quando for provocado por uso inadequado.

6.2. Suporte Técnico:

6.2.1. Durante a vigência deste Contrato deverá ser fornecido suporte técnico pela CONTRATADA seguindo as especificações abaixo:

6.2.1.1. Apoio às respostas a incidentes de segurança envolvendo malware;

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

6.2.1.3. Acompanhamento nos chamados escalados para a Fabricante em situações de falhas/problemas desconhecidos pelo suporte técnico da CONTRATADA ou bugs;

6.2.1.4. O atendimento deverá ser realizado via contato telefônico ou ferramenta de acesso remoto independentemente do tipo de incidente;

6.2.1.5. Suporte técnico telefônico fornecido em horário comercial de segunda a sexta-feira das 8h às 18h prestado unicamente à equipe de segurança da área de informática do CONTRATANTE referente a problemas de funcionamento/configuração dos produtos fornecidos;

6.2.1.6. Número de chamados ilimitados; e

6.2.1.7. Tempo de atendimento telefônico máximo de duas horas após a abertura do chamado técnico.

6.2.2. Incidentes, chamados, e problemas escalados ao Fabricante deverão ter o acordo de nível de serviço (SLA) conforme tabela abaixo:

NÍVEIS DE SEVERIDADE	DESCRIÇÃO	PRAZO PARA SOLUÇÃO
Nível 1 - Crítico	Afeta o serviço prestado pelo Contratante por interrupções da solução de antivírus nos sistemas operacionais, possíveis perda de dados, alterações de configuração padrão para configuração insegura e onde não há solução alternativa disponível.	6 horas
Nível 2 - Alto	Afeta a funcionalidade do produto, mas não causa corrupção e perda de dados ou travamento sistemas.	10 horas
Nível 3 - Médio	Solicitações não críticas, as quais não afetam a funcionalidade do produto.	12 horas
Nível 4 - Baixo	Solicitações não críticas ou solicitação de serviços. Todos os incidentes que não satisfaçam um dos critérios listados acima, serão classificados a esse nível de gravidade.	14 horas

6.3. Será respeitado o horário de expediente do CONTRATANTE, caso o prazo de solução expire em horário não comercial, a contagem do prazo de solução será paralisada no final do expediente e iniciada no próximo dia útil, contando o prazo de solução já decorrido do chamando no dia anterior.

CLÁUSULA SÉTIMA – DO VALOR:

7.1. O valor ordinário do presente Instrumento fica ajustado em **RS 55.550,00 (cinquenta e cinco mil quinhentos e cinquenta reais)**, compreendendo todas as despesas e custos diretos e indiretos necessários à perfeita execução deste Contrato.

CLÁUSULA OITAVA – DA DOTAÇÃO ORÇAMENTÁRIA:

8.1. 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: 33.90.30

Fonte de Recursos: 0100

8.2. 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.

8.3. A CONTRATADA emitirá Nota Fiscal em observância à unidade gestora emissora da nota de empenho que albergou a aquisição.

CLÁUSULA NONA – DO PAGAMENTO:

9.1. A CONTRATADA deverá, obrigatoriamente, apresentar nota fiscal correspondente as licenças renovação e/ou aquisição.

9.2. A nota fiscal/fatura deverá indicar o número da conta corrente e agência bancária para emissão da respectiva Ordem Bancária, além do número da nota de empenho.

9.3. Caso tenha ocorrido o fornecimento de objetos importados, juntamente com a nota fiscal/fatura deverá ser apresentado documento que comprove a origem dos objetos e a quitação dos tributos de importação a eles referentes, se for o caso, sob pena de rescisão contratual e multa.

9.4. Sobre a fatura incidirão os tributos legalmente instituídos e as multas que eventualmente vierem a ser aplicadas. Sendo a CONTRATADA isenta ou beneficiária de redução de alíquota de qualquer imposto, taxa ou de contribuição social ou ainda optante pelo SIMPLES, deverá apresentar junto com a fatura, cópia do comprovante respectivo.

9.5. O CONTRATANTE, por meio do gestor do contrato, 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 Contrato, Ata e no Termo de Referência, ficando o pagamento suspenso até a regularização.

9.6. O atesto do(a) gestor(a) do contrato na nota fiscal é condição indispensável para o pagamento.

9.7. Na ausência do fiscal do contrato (férias, licença ou em viagem por interesse do CONTRATANTE, o atesto será dado pelo gestor substituto.

9.8. 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: **Banco - 104, Caixa Econômica Federal, Agência nº 1585, Conta Corrente nº 2852-4 - Operação: 003.**

9.9. O CNPJ constante da Nota Fiscal deverá ser o mesmo indicado na proposta e Nota de Empenho.

9.10. Fica a CONTRATADA ciente que por ocasião do pagamento será verificada sua situação quanto à regularidade fiscal exigida na habilitação, as quais deverão ser mantidas durante toda a execução contratual.

9.11. Ocorrendo atraso no pagamento, e desde que tal não tenha concorrido de alguma forma a 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.

9.12. Todos os atos inerentes ao presente processo obedecerão às regras concernentes ao Sistema Eletrônico de Informações – SEI do CONTRATANTE.

CLÁUSULA DÉCIMA - DAS OBRIGAÇÕES DA CONTRATADA:

10.1. A CONTRATADA obriga-se à:

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. Atender prontamente às solicitações do CONTRATANTE no fornecimento dos objetos nas quantidades e especificações constantes neste Instrumento, Ata de Registro de Preços e no Termo de Referência, a partir da solicitação do gestor do contrato;

10.1.3. 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, de 1993, incluindo a atualização de documentos de controle da arrecadação de tributos e contribuições federais e outras legalmente exigíveis;

10.1.4. 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 desta contratação;

10.1.5. Indicar, formalmente, preposto apto a representá-la junto ao CONTRATANTE, que deverá responder pela fiel execução deste Contrato;

10.1.6. Prestar todos os esclarecimentos técnicos que lhe forem solicitados pelo CONTRATANTE, relacionados com as características e funcionamento dos objetos, inclusive em relação aos problemas detectados;

10.1.7. Comunicar, imediatamente, por escrito qualquer anormalidade, prestando ao CONTRATANTE os esclarecimentos julgados necessários;

10.1.8. Manter, durante a execução deste Contrato, equipe técnica composta por profissionais devidamente habilitados; treinados e qualificados para prestação dos serviços;

10.1.9. Manter ficha de controle do serviço, na qual serão relatadas todas as ocorrências;

10.1.10. Assumir inteira responsabilidade técnica e operacional, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas no fornecimento do objeto deste Contrato;

10.1.11. Não transferir a outrem, no todo ou em parte, o objeto desta prestação.

10.1.12. Identificar qualquer equipamento de sua posse que venha a ser utilizado nas dependências do CONTRATANTE, afixando placas de controle patrimonial, selos de segurança etc;

10.1.13. 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;

10.1.14. Cumprir integralmente as exigências do Acordo de Nível de Serviço, disposto no “Anexo C” do Termo de Referência;

10.1.15. 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.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DO CONTRATANTE:

11.1. O CONTRATANTE obriga-se a:

11.1.1. Observar as leis, decretos, regulamentos, portarias e normas legais, estaduais e municipais direta e indiretamente aplicáveis ao objeto deste Contrato;

11.1.2. Receber os objetos de acordo com as disposições deste Contrato, Ata de Registro de Preços e do Termo de Referência;

11.1.3. Comunicar imediatamente a CONTRATADA qualquer incorreção apresentada com os objetos entregues;

11.1.4. Solicitar a imediata substituição de qualquer objeto que não atendam as exigências contratuais;

11.1.5. Rejeitar, no todo ou em parte, os objetos fornecidos em desacordo com as especificações deste Instrumento e do Termo de Referência;

11.1.6. Acompanhar e fiscalizar a execução deste Contrato, por meio de servidor especialmente designado;

11.1.7. Responsabilizar-se pela lavratura do respectivo contrato, com base nas disposições da Lei;

11.1.8. Assegurar os recursos orçamentários e financeiros para custear os bens adquiridos e promover os pagamentos dentro dos prazos convencionados neste Contrato;

11.1.9. Processar e liquidar a fatura correspondente aos valores, por meio de ordem bancária, desde que não haja fatoa impeditivos imputados à CONTRATADA;

11.1.10. 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 SEGUNDA – DAS SANÇÕES ADMINISTRATIVAS:

12.1. 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 Cadastro 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.

12.2. Subsidiariamente, nos termos do art. 87 da Lei nº. 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 empresa deixar de atender quaisquer indicações aqui constantes;
- b) Multa compensatória/indenizatória no percentual de 5% (cinco por cento) calculado sobre o valor contratado;
- c) Suspensão temporária de participação em licitação e impedimento de contratar com o Poder Judiciário do Estado do Tocantins, pelo prazo de até 2 (dois) anos; e
- d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

12.3. 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.

12.4. 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;

12.5. Caso não seja paga no prazo previsto no subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado pelo CONTRATANTE ou cobrada judicialmente.

12.6. 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 TERCEIRA – DA RESCISÃO:

13.1. 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.

CLÁUSULA DÉCIMA QUARTA – DA VINCULAÇÃO:

14.1. O presente Contrato fica vinculado aos autos 19.0.00003897-3 e 19.0.000031831-3 .

CLÁUSULA DÉCIMA QUINTA – DA LEGISLAÇÃO E CASOS OMISSOS:

15.1. O presente Instrumento, inclusive os casos omissos, regula-se pela Lei nº 10.520/2002, pelo Decreto nº 5.450/2005 e, subsidiariamente, pela Lei nº 8.666/1993 e suas alterações.

CLÁUSULA DÉCIMA SEXTA – DA VIGÊNCIA:

16.1. O presente Contrato terá a vigência de 24 (vinte quatro) meses, contados a partir da data do recebimento definitivo das licenças, ressalvado o prazo de garantia dos objetos.

CLÁUSULA DÉCIMA SÉTIMA – DA SUBCONTRATAÇÃO:

17.1. É vedado, no todo ou em parte, a subcontratação do objeto deste Contrato pela CONTRATADA.

CLÁUSULA DÉCIMA OITAVA – DA PUBLICAÇÃO:

18.1. A publicação resumida deste Contrato no Diário da Justiça Eletrônico - 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 NONA – DA GESTÃO E FISCALIZAÇÃO:

19.1. A gestão e fiscalização deste Contrato ficarão a cargo da Diretoria de Tecnologia da Informação do CONTRATANTE.

19.2. Profissionais da CONTRATADA: equipe composta por técnicos, responsáveis pela execução e acompanhamento do objeto.

19.2.1. Técnico: funcionário da CONTRATADA, responsável pela execução técnica-operacional.

19.2.2. 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.

19.3. 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.

19.3.1. 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.

19.3.2. 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.

19.3.3. 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.

19.3.4. 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.

19.4. 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 objetos.

19.5. 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.

19.6. A comunicação entre a fiscalização e da CONTRATADA será realizada por meio de correspondência oficial e anotações ou registros no mesmo processo que tratam da aquisição dos objetos.

19.7. Quando houver necessidade o gestor deverá emitir notificações para a CONTRATADA.

CLÁUSULA VIGÉSIMA – DAS DISPOSIÇÕES GERAIS:

20.1. Não será permitida direta ou indiretamente cobrança retroativa de valores relativos aos serviços de suporte técnico e de atualização de versões.

20.2. Não será permitida direta ou indiretamente a cobrança de valores relativos a serviço de correção de erros, inclusive retroativos, de modo que o fabricante entregue correções dos softwares licenciados sem ônus, dentro do prazo de validade técnica dos softwares licenciados e, se o erro somente for corrigido em versão posterior do software, que essa versão seja fornecida sem ônus para a organização pública.

20.3. Não será permitida direta ou indiretamente permita a cobrança de taxa específica para o restabelecimento dos serviços agregados.

CLÁUSULA VIGÉSIMA PRIMEIRA – DO FORO:

21.1. Para dirimir todas as questões oriundas 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, lavrou-se o presente Termo que, depois de lido e achado conforme, vai assinado pelas partes contratantes, por meio de assinatura eletrônica utilizando-se do Sistema Eletrônico de Informação – SEI.



Documento assinado eletronicamente por **Dennis Fernandes de Medeiros, Usuário Externo**, em 08/10/2019, às 18:41, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Jonas Demostene Ramos, Diretor Geral**, em 10/10/2019, às 18:03, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no link <http://sei.tjto.jus.br/verifica/> informando o código verificador **2829949** e o código CRC **70369B48**.