TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

# TERMO DE REFERÊNCIA

## 1. OBJETO

1.1. Fornecimento de Solução para Proteção de Endpoints - Kaspersky, bem como serviços de instalação, configuração, treinamento, prestação de consultoria e suporte técnico em sistemas de segurança na solução fornecida para prevenção de vírus de computador, spywares e outras ameaças digitais, por um período de 36 meses (trina e seis meses), para atender ao Tribunal de Justiça do Estado do Amazonas.

## 2. JUSTIFICATIVA

2.1. O TJAM atualmente disponibiliza uma gama de serviços e aplicações internas para os seus servidores, estas operações são fundamentais para o funcionamento deste Tribunal e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de paradas e o impacto negativo sobre o desempenho institucional.
2.2. A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que este Tribunal mantenha as operações de segurança em níveis de risco admissíveis.
2.3. Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.
2.4. Mesmo diante deste cenário de ataques cibernéticos, o TJAM está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.
2.5. Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas neste Tribunal, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.
2.6. Cabe ressaltar o comprometimento por parte deste Tribunal a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em “adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”.
2.7. Mediante ao exposto, é necessária a aquisição de uma Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado neste tribunal e reforçar a segurança digital do ambiente, com a prevenção de vírus de computador, spyware, ransomware e outras ameaças digitais.

## 3. FUNDAMENTAÇÂO LEGAL

3.1. A contratação para a execução dos serviços deverá obedecer, no que couber, ao disposto na Lei nº. 8.666/93, de 21 de junho de 1993 e suas alterações, bem como nas seguintes normas:
3.1.1. Lei n°10.520, de 17 de julho de 2002;
3.1.2. Decreto Estadual nº. 40.674/2019;

3.1.3. Decreto nº 7.892, de 23 de janeiro de 2013;
3.1.4. Resolução nº 25/2019 - TJAM;

3.1.5. Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados.

## 4. DO REGISTRO DE PREÇOS E CRITÉRIO DE JULGAMENTO

4.1 O objeto do presente Termo de Referência resultará em adesão a ata de registro de preços;

4.2 O critério de julgamento do certame será o de menor preço global.

## 5. ESPECIFICAÇÃO DO OBJETO

5.1. Servidor de Administração e Console Administrativa
5.1.1. Compatibilidade:
5.1.1.1. Microsoft Storage Server 2012 e 2012 R2 x64;
5.1.1.2. Microsoft Windows Server 2012 Standard / Core / Foundation / Essentials / Datacenter x64;
5.1.1.3. Microsoft Windows Server 2012 R2 Standard / Core / Foundation / Essentials / Datacenter x64;
5.1.1.4. Microsoft Windows Server 2016 Standard / Core / Datacenter x64;
5.1.1.5. Microsoft Windows Server 2019 Standard / Core / Datacenter x64;
5.1.1.6. Microsoft Windows Server 2022 Standard / Core / Datacenter x64;
5.1.1.7. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
5.1.1.8. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
5.1.1.9. Microsoft Windows 8 Professional / Enterprise x64;
5.1.1.10. Microsoft Windows 8.1 Professional / Enterprise x32;
5.1.1.11. Microsoft Windows 8.1 Professional / Enterprise x64;
5.1.1.12. Microsoft Windows 10 x32;
5.1.1.13. Microsoft Windows 10 x64;
5.1.1.14. Windows 10 21H1 31-bit/64-bit;
5.1.1.15. Microsoft Windows 11 Home / Pro / Enterprise /Education 64 bits
5.1.2. Suporta as seguintes plataformas virtuais:
5.1.2.1. Vmware: Workstation 16.x Pro, vSphere 6.7, vSphere 7.0;
5.1.2.2. Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64;
5.1.2.3. Parallels Desktop 17;
5.1.2.4. Citrix XenServer 7.1LTSR e 8;
5.1.3. Características:
5.1.3.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
5.1.3.2. A console deve suportar arquitetura on-premise e arquitetura cloud-based;
5.1.3.3. Console deve ser baseada no modelo cliente/servidor;
5.1.3.4. A console deve suportar autênticação de dois fatores;
5.1.3.5. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
5.1.3.6. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
5.1.3.7. Deve permitir incluir usuários do AD para logarem na console de administração
5.1.3.8. 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;
5.1.3.9. 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;
5.1.3.10. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
5.1.3.11. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD.
5.1.3.12. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
5.1.3.13. Deve armazenar histórico das alterações feitas em políticas;
5.1.3.14. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
5.1.3.15. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

5.1.3.16. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
5.1.3.17. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
5.1.3.18. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
5.1.3.19. 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;
5.1.3.20. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
5.1.3.21. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
5.1.3.22. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
5.1.3.23. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
5.1.3.24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
5.1.3.25. 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;
5.1.3.26. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
5.1.3.27. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
5.1.3.28. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:
5.1.3.28.1. Nome do computador;
5.1.3.28.2. Nome do domínio;
5.1.3.28.3. Range de IP;
5.1.3.28.4. Sistema Operacional;
5.1.3.28.5. Máquina virtual.
5.1.3.29. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
5.1.3.30. 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;
5.1.3.31. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
5.1.3.32. 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;
5.1.3.33. 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;
5.1.3.34. 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;
5.1.3.35. 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;
5.1.3.36. Deve fornecer as seguintes informações dos computadores:
5.1.3.36.1. Se o antivírus está instalado;
5.1.3.36.2. Se o antivírus está iniciado;
5.1.3.36.3. Se o antivírus está atualizado;
5.1.3.36.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
5.1.3.36.5. Minutos/horas desde a última atualização de vacinas;
5.1.3.36.6. Data e horário da última verificação executada na máquina
5.1.3.36.7. Versão do antivírus instalado na máquina;
5.1.3.36.8. Se é necessário reiniciar o computador para aplicar mudanças;
5.1.3.36.9. Data e horário de quando a máquina foi ligada;
5.1.3.36.10. Quantidade de vírus encontrados (contador) na máquina;
5.1.3.36.11. Nome do computador;
5.1.3.36.12. Domínio ou grupo de trabalho do computador;
5.1.3.36.13. Data e horário da última atualização de vacinas;

5.1.3.36.14. Sistema operacional com Service Pack;
5.1.3.36.15. Quantidade de processadores;
5.1.3.36.16. Quantidade de memória RAM;
5.1.3.36.17. Sessões de usuários, com informações de contato (caso disponíveis no Active Directory);
5.1.3.36.18. Endereço IP;
5.1.3.36.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
5.1.3.36.20. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
5.1.3.36.21. Vulnerabilidades de aplicativos instalados na máquina;
5.1.3.37. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
5.1.3.38. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
5.1.3.38.1. Disponibilidade de endereço de conexão SSL;
5.1.3.38.2. Resolução de Nome;
5.1.3.38.3. Alteração de subrede;
5.1.3.38.4. Alteração de servidor WINS;
5.1.3.38.5. Alteração de servidor DNS;
5.1.3.38.6. Alteração de servidor DHCP;
5.1.3.38.7. Alteração de domínio;
5.1.3.38.8. Alteração de subrede;
5.1.3.38.9. Alteração de Gateway Padrão;
5.1.3.39. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
5.1.3.40. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
5.1.3.41. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
5.1.3.42. A console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores;
5.1.3.43. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
5.1.3.44. 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;
5.1.3.45. 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;
5.1.3.46. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
5.1.3.47. Capacidade de monitoramento do sistema através de um SNMP client;
5.1.3.48. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
5.1.3.49. Listar em um único local, todos os computadores não gerenciados na rede;
5.1.3.50. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
5.1.3.51. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
5.1.3.52. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente
5.1.3.53. 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;
5.1.3.54. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
5.1.3.55. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;
5.1.3.56. 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);
5.1.3.57. 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;

5.1.3.58. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
5.1.3.59. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
5.1.3.60. Capacidade de listar updates nas máquinas com o respectivo link para download
5.1.3.61. Deve criar um backup de todos arquivos deletados em computadores durante a desinfecção para que possam ser restaurados;
5.1.3.62. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
5.1.3.63. Capacidade de realizar resumo de hardware de cada máquina cliente;
5.1.3.64. Capacidade de realizar resumo de hardware de cada máquina cliente;
5.1.3.65. Capacidade de diferenciar máquinas virtuais de máquinas físicas.
5.1.3.66. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
5.1.3.66.1. Nome do vírus;
5.1.3.66.2. Nome do arquivo infectado;
5.1.3.66.3. Data e hora da detecção;
5.1.3.66.4. Nome da máquina ou endereço IP;
5.1.3.66.5. Ação realizada.
5.2. Estações Windows
5.2.1. Compatibilidade:
5.2.1.1. Microsoft Windows 7 Professional/Enterprise/Home SP1 x86 / x64;
5.2.1.2. Microsoft Windows 8 Professional/Enterprise x86 / x64; 2.1.3.Microsoft Windows 8.1 Professional / Enterprise x86 / x64; 2.1.4.Microsoft Windows 10 Pro / Enterprise / Home / Education x86 / x64; 2.1.5.Microsoft Windows 11;
5.2.1.3. Microsoft Windows Server 2019 Essentials / Standard / Datacenter; 2.1.7.Microsoft Windows Server 2016 Essentials / Standard / Datacenter; 2.1.8.Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard /Datacenter;
5.2.1.4. Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
5.2.1.5. Microsoft Windows Server 2008 R2 Foundation / Essentials / Standard / Datacenter SP1;
5.2.1.6. Microsoft Windows MultiPoint Server 2011 x64;
5.2.1.7. Microsoft Windows Server 2022.
5.2.2. Características:
5.2.2.1. Deve prover as seguintes proteções:
5.2.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti- malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
5.2.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
5.2.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
5.2.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
5.2.2.1.5. Firewall com IDS;
5.2.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);
5.2.2.1.7. Controle de dispositivos externos;
5.2.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
5.2.2.1.9. Controle de acesso a sites por horário;
5.2.2.1.10. Controle de acesso a sites por usuários;
5.2.2.1.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
5.2.2.1.12. Controle de execução de aplicativos;
5.2.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
5.2.2.1.14. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.2.2.1.15. 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);
5.2.2.1.16. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5.2.2.1.17. 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;

5.2.2.1.18. 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;
5.2.2.1.19. Deverá possuir módulo dedicado para proteção contra port scanning;
5.2.2.1.20. Deverá possuir módulo dedicado para proteção contra network flooding;
5.2.2.1.21. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
5.2.2.1.22. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
5.2.2.1.23. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
5.2.2.1.24. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
5.2.2.1.25. Ao detectar uma ameaça, a solução deve exibir informações:
5.2.2.1.25.1. Do objeto SHA256;
5.2.2.1.25.2. Do objeto MD5
5.2.2.1.26. Capacidade de verificar somente arquivos novos e alterados;
5.2.2.1.27. Capacidade de verificar objetos usando heurística;
5.2.2.1.28. Capacidade de agendar uma pausa na verificação;
5.2.2.1.29. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
5.2.2.1.30. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
5.2.2.1.31. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
5.2.2.1.31.1. Perguntar o que fazer, ou;
5.2.2.1.31.2. Bloquear acesso ao objeto;
5.2.2.1.31.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
5.2.2.1.31.2.2. Caso positivo de desinfecção:
5.2.2.1.31.2.2.1. Restaurar o objeto para uso;
5.2.2.1.31.2.3. Caso negativo de desinfecção:
5.2.2.1.31.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
5.2.2.1.32. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
5.2.2.1.33. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;
5.2.2.1.34. Capacidade de verificar links inseridos em e-mails contra phishings;
5.2.2.1.35. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
5.2.2.1.36. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
5.2.2.1.37. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
5.2.2.1.37.1. Perguntar o que fazer, ou;
5.2.2.1.37.2. Bloquear o e-mail;
5.2.2.1.37.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
5.2.2.1.37.2.2. Caso positivo de desinfecção:
5.2.2.1.37.2.2.1. Restaurar o e-mail para o usuário;
5.2.2.1.37.2.3. Caso negativo de desinfecção:
5.2.2.1.37.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
5.2.2.1.38. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
5.2.2.1.39. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
5.2.2.1.40. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
5.2.2.1.41. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
5.2.2.1.42. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
5.2.2.1.42.1. Perguntar o que fazer, ou;

5.2.2.1.42.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
5.2.2.1.42.3. Permitir acesso ao objeto;
5.2.2.1.43. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
5.2.2.1.43.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
5.2.2.1.43.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
5.2.2.1.44. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
5.2.2.1.45. 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;
5.2.2.1.46. 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;
5.2.2.1.47. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);
5.2.2.1.48. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
5.2.2.1.49. 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;
5.2.2.1.50. Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;
5.2.2.1.51. Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.
5.2.2.1.52. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
5.2.2.1.52.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
5.2.2.1.52.2. 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.
5.2.2.1.53. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
5.2.2.1.53.1. Discos de armazenamento locais;
5.2.2.1.53.2. Armazenamento removível;
5.2.2.1.53.3. Impressoras;
5.2.2.1.53.4. CD/DVD;
5.2.2.1.53.5. Drives de disquete;
5.2.2.1.53.6. Modems;
5.2.2.1.53.7. Dispositivos de fita;
5.2.2.1.53.8. Dispositivos multifuncionais;
5.2.2.1.53.9. Leitores de smart card;
5.2.2.1.53.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
5.2.2.1.53.11. Wi-Fi;
5.2.2.1.53.12. Adaptadores de rede externos;
5.2.2.1.53.13. Dispositivos MP3 ou smartphones;
5.2.2.1.53.14. Dispositivos Bluetooth;
5.2.2.1.53.15. Câmeras e Scanners.
5.2.2.1.54. 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;
5.2.2.1.55. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
5.2.2.1.56. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
5.2.2.1.57. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras.
5.2.2.1.58. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.
5.2.2.1.59. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
5.2.2.1.60. 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);
5.2.2.1.61. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:
5.2.2.1.61.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
5.2.2.1.61.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
5.2.2.1.62. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
5.2.2.1.63. 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;
5.2.2.1.64. 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;
5.2.2.1.65. 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.
5.2.2.1.66. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.
5.2.2.1.67. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
5.2.2.1.68. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
5.2.2.1.69. Capacidade de integração com o Windows Defender Security Center.
5.2.2.1.70. Capacidade de integração com a Antimalware Scan Interface (AMSI).
5.2.2.1.71. Deve permitir sincronização com soluções de terceiros por meio de API.
5.2.2.1.72. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.
5.3. Estações Mac OS X
5.3.1. Compatibilidade:
5.3.1.1. macOS Catalina 10.15
5.3.1.2. macOS Mojave 10.14
5.3.1.3. macOS High Sierra 10.13
5.3.1.4. macOS Sierra 10.12
5.3.1.5. macOS 11.0 Big Sur
5.3.2. Características:
5.3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti- malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
5.3.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https;
5.3.2.3. Possuir módulo de bloqueio á ataques na rede;
5.3.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
5.3.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
5.3.2.6. Possibilidade de importar uma chave no pacote de instalação;
5.3.2.7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.3.2.8. 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);
5.3.2.9. Capacidade de voltar para a base de dados de vacina anterior;
5.3.2.10. 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;
5.3.2.11. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
5.3.2.12. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
5.3.2.13. Capacidade de verificar somente arquivos novos e alterados;
5.3.2.14. Capacidade de verificar objetos usando heurística;
5.3.2.15. Capacidade de agendar uma pausa na verificação;

5.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
5.3.2.16.1. Perguntar o que fazer, ou;
5.3.2.16.2. Bloquear acesso ao objeto;
5.3.2.16.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
5.3.2.16.3.1. Caso positivo de desinfecção:
5.3.2.16.3.1.1. Restaurar o objeto para uso;
5.3.2.16.3.2. Caso negativo de desinfecção:
5.3.2.16.3.2.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
5.3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
5.3.2.18. Capacidade de verificar arquivos de formato de e-mail;
5.3.2.19. 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;
5.3.2.20. Capacidade de, através da mesma console central de gerenciamento:
5.3.2.20.1. Ser instalado;
5.3.2.20.2. Ser removido;
5.3.2.20.3. Ser gerenciado;
5.4. Estações de trabalho Linux
5.4.1. Compatibilidade:
5.4.1.1. Plataforma 32-bits:
5.4.1.1.1. Red Hat® Enterprise Linux® 6.7 Server;
5.4.1.1.2. CentOS 6.7;
5.4.1.1.3. Debian GNU / Linux 9.4 ;
5.4.1.1.4. Debian GNU / Linux 10.1;
5.4.1.1.5. Debian GNU / Linux 11.1;
5.4.1.1.6. Linux Mint 18.2;
5.4.1.1.7. Linux Mint 19;
5.4.1.1.8. GosLinux 6.6;
5.4.1.1.9. Mageia 4;
5.4.1.2. Plataforma 64-bits:
5.4.1.2.1. Ubuntu 18.04 LTS;
5.4.1.2.2. Ubuntu 20.04 LTS;
5.4.1.2.3. Red Hat Enterprise Linux 6.7;
5.4.1.2.4. Red Hat Enterprise Linux 7.2;
5.4.1.2.5. Red Hat Enterprise Linux 8.0;
5.4.1.2.6. CentOS 6.7;
5.4.1.2.7. CentOS 7.2;
5.4.1.2.8. CentOS 8.0;
5.4.1.2.9. Debian GNU / Linux 9.4
5.4.1.2.10. Debian GNU / Linux 10.1;
5.4.1.2.11. Debian GNU / Linux 11.1;
5.4.1.2.12. OracleLinux 7.3;
5.4.1.2.13. OracleLinux 8;
5.4.1.2.14. SUSE® Linux Enterprise Server 15;
5.4.1.2.15. openSUSE® Leap 15;
5.4.1.2.16. Amazon Linux AMI
5.4.1.2.17. Linux Mint 19;
5.4.1.2.18. Linux Mint 20.1;
5.4.1.2.19. GosLinux 7.2
5.4.1.2.20. SUSE Linux Enterprise Server 12 SP5;
5.4.1.2.21. Pardus OS 19.1;
5.4.1.2.22. RED OS 7.3.
5.4.2. Características:
5.4.2.1. Deve prover as seguintes proteções:
5.4.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

5.4.2.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:
5.4.2.3.1. Via linha de comando;
5.4.2.3.2. Via console administrativa;
5.4.2.3.3. Via GUI;
5.4.2.3.4. Via web (remotamente);
5.4.2.4. Deve possuir funcionalidade de scan de drives removíveis, tais como:
5.4.2.4.1. CDs;
5.4.2.4.2. DVDs;
5.4.2.4.3. Discos blu-ray;
5.4.2.4.4. Flash drives (pen drives);
5.4.2.4.5. HDs externos;
5.4.2.4.6. Disquetes;
5.4.2.5. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:
5.4.2.5.1. Por tipo de dispositivo;
5.4.2.5.2. Por barramento de conexão.
5.4.2.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
5.4.2.7. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
5.4.2.8. Capacidade de criar exclusões por local, máscara e nome da ameaça;
5
5.2.9.Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
5.4.3. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
5.4.4. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
5.4.5. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
5.4.5.1. Alta;
5.4.5.2. Média;
5.4.5.3. Baixa;
5.4.5.4. Recomendado;
5.4.6. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
5.4.7. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
5.4.8. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
5.4.9. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
5.4.10. Capacidade de verificar objetos usando heurística;
5.4.11. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
5.4.12. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP que chegar no computador do usuário.
5.4.13. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:
5.4.13.1. Detecção de phishing e sites maliciosos;
5.4.13.2. Bloqueio de download de arquivos maliciosos;
5.4.13.3. Bloqueio de adware;
5.4.14. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
5.4.15. Deve fornecer a possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
5.4.16. Deve possuir módulo de proteção contra criptografia maliciosa.
5.5. Servidores Windows
5.5.1. Compatibilidade:
5.5.1.1. Plataforma 32-bits:
5.5.1.1.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
5.5.1.1.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
5.5.1.1.3. Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior;
5.5.1.1.4. Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior.
5.5.1.2. Plataforma 64-bits

5.5.1.2.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
5.5.1.2.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
5.5.1.2.3. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter SP1 ou 5osterior;
5.5.1.2.4. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter SP1 ou posterior.
5.5.1.2.5. Microsoft Windows Server 2008 R2 Foundation / Standard / Enterprise / DataCenter SP1 ou posterior;
5.5.1.2.6. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter SP1 ou posterior;
5.5.1.2.7. Microsoft Small Business Server 2008 Standard / Premium
5.5.1.2.8. Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;
5.5.1.2.9. Microsoft Microsoft Small Business Server 2011 Essentials / Standard
5.5.1.2.10. Microsoft Windows MultiPoint Server 2011;
5.5.1.2.11. Microsoft MultiPoint Server 2012 Standard / Premium;
5.5.1.2.12. Microsoft Windows MultiPoint Server 2016
5.5.1.2.13. Windows 10 Enterprise multi-session;
5.5.1.2.14. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
5.5.1.2.15. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
5.5.1.2.16. Microsoft Windows Server 2012 Core Standard / Datacenter;
5.5.1.2.17. Microsoft Windows Server 2012 R2 Core Standard / Datacenter;
5.5.1.2.18. Microsoft Windows Storage Server 2012;
5.5.1.2.19. Microsoft Windows Storage Server 2012 R2;
5.5.1.2.20. Microsoft Windows Hyper-V Server 2012;
5.5.1.2.21. Microsoft Windows Hyper-V Server 2012 R2;
5.5.1.2.22. Windows Server 2016 Essentials /Standard / Datacenter;
5.5.1.2.23. Windows Server 2016 Core Standard / Datacenter;
5.5.1.2.24. Windows Storage Server 2016;
5.5.1.2.25. Windows Storage Server 2019;
5.5.1.2.26. Windows Hyper-V Server 2016;
5.5.1.2.27. Windows Hyper-V Server 2019;
5.5.1.2.28. Windows Server 2019 Essentials / Standard / Datacenter / Core / Terminal;
5.5.2. Características:
5.5.2.1. Deve prover as seguintes proteções:
5.5.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti- malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
5.5.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;
5.5.2.1.3. Firewall com IDS;
5.5.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
5.5.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.5.2.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:
5.5.2.3.1. Via console administrativa;
5.5.2.3.2. Via web (remotamente);
5.5.2.4. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
5.5.2.5. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
5.5.2.5.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
5.5.2.5.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
5.5.2.5.3. Leitura de configurações;
5.5.2.5.4. Modificação de configurações;
5.5.2.5.5. Gerenciamento de Backup e Quarentena;
5.5.2.5.6. Visualização de logs;
5.5.2.5.7. Gerenciamento de logs;
5.5.2.5.8. Gerenciamento de ativação da aplicação;
5.5.2.5.9. Gerenciamento de permissões (adicionar/excluir permissões acima);
5.5.2.5.10. Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.
5.5.2.6. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
5.5.2.6.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

5.5.2.6.2. 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.
5.5.2.7. 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;
5.5.2.8. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;
5.5.2.9. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
5.5.2.10. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
5.5.2.11. Deve possuir funcionalidade de análise personalizada de logs do Windows.
5.5.2.12. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
5.5.2.13. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
5.5.2.14. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
5.5.2.15. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5.5.2.16. 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;
5.5.2.17. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
5.5.2.18. Capacidade de verificar somente arquivos novos e alterados;
5.5.2.19. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
5.5.2.20. Capacidade de verificar objetos usando heurística;
5.5.2.21. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
5.5.2.22. Capacidade de agendar uma pausa na verificação;
5.5.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
5.5.2.23.1. Perguntar o que fazer, ou;
5.5.2.23.2. Bloquear acesso ao objeto;
5.5.2.23.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
5.5.2.23.4. Caso positivo de desinfecção:
5.5.2.23.4.1. Restaurar o objeto para uso;
5.5.2.23.5. Caso negativo de desinfecção:
5.5.2.23.5.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
5.5.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
5.5.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
5.5.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
5.5.2.27. Em caso de detecção de sinais de de uma infecção ativa, deve possuir capacidade de, automaticamente:
5.5.2.28. Executar os procedimentos pré-configurados pelo administrador;
5.5.2.29. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.
5.5.2.30. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
5.5.2.31. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros
5.5.2.32. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
5.5.2.33. 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.

5.5.2.34. Deve possuir controle de dispositivos externos.
5.6. Servidores Linux
5.6.1. Compatibilidade:
5.6.1.1. Plataforma 32-bits:
5.6.1.1.1. Red Hat® Enterprise Linux® 6.7 Server;
5.6.1.1.2. CentOS 6.7;
5.6.1.1.3. Debian GNU / Linux 9.4 ;
5.6.1.1.4. Debian GNU / Linux 10.1;
5.6.1.1.5. Debian GNU / Linux 11.1;
5.6.1.1.6. Linux Mint 18.2;
5.6.1.1.7. Linux Mint 19;
5.6.1.1.8. GosLinux 6.6;
5.6.1.1.9. Mageia 4;
5.6.1.2. Plataforma 64-bits:
5.6.1.2.1. Ubuntu 18.04 LTS;
5.6.1.2.2. Ubuntu 20.04 LTS;
5.6.1.2.3. Red Hat Enterprise Linux 6.7;
5.6.1.2.4. Red Hat Enterprise Linux 7.2;
5.6.1.2.5. Red Hat Enterprise Linux 8.0;
5.6.1.2.6. CentOS 6.7;
5.6.1.2.7. CentOS 7.2;
5.6.1.2.8. CentOS 8.0;
5.6.1.2.9. Debian GNU / Linux 9.4
5.6.1.2.10. Debian GNU / Linux 10.1;
5.6.1.2.11. Debian GNU / Linux 11.1;
5.6.1.2.12. OracleLinux 7.3;
5.6.1.2.13. OracleLinux 8;
5.6.1.2.14. SUSE® Linux Enterprise Server 15;
5.6.1.2.15. openSUSE® Leap 15;
5.6.1.2.16. Amazon Linux AMI
5.6.1.2.17. Linux Mint 19;
5.6.1.2.18. Linux Mint 20.1;
5.6.1.2.19. GosLinux 7.2
5.6.1.2.20. SUSE Linux Enterprise Server 12 SP5;
5.6.1.2.21. Pardus OS 19.1;
5.6.1.2.22. RED OS 7.3;
5.6.2. Características:
5.6.2.1. Deve prover as seguintes proteções:
5.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
5.6.2.2. Deve permitir gerenciamento, no mínimo, das seguintes formas:
5.6.2.2.1. Via linha de comando;
5.6.2.2.2. Via console administrativa;
5.6.2.2.3. Via GUI;
5.6.2.2.4. Via web;
5.6.2.3. Deve possuir funcionalidade de scan de drives removíveis, tais como:
5.6.2.3.1. CDs;
5.6.2.3.2. DVDs;
5.6.2.3.3. Discos Blu-ray;
5.6.2.3.4. Flash drives;
5.6.2.3.5. HDs externos;
5.6.2.3.6. Disquetes;
5.6.2.4. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:
5.6.2.4.1. Por tipo de dispositivo;
5.6.2.4.2. Por barramento de conexão.
5.6.2.5. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
5.6.2.6. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
5.6.2.7. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup

antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
5.6.2.8. Gerenciamento de Quarentena: Deve bloquear objetos suspeitos;
5.6.2.9. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados);
5.6.2.10. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
5.6.2.11. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
5.6.2.12. Capacidade de verificar objetos usando heurística;
5.6.2.13. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
5.6.2.14. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
5.6.2.14.1. Alta;
5.6.2.14.2. Média;
5.6.2.14.3. Baixa;
5.6.2.14.4. Recomendado;
5.6.2.15. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP que chegar no computador do usuário.
5.6.2.16. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:
5.6.2.16.1. Detecção de phishing e sites maliciosos;
5.6.2.16.2. Bloqueio de download de arquivos maliciosos;
5.6.2.16.3. Bloqueio de adware;
5.6.2.17. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
5.6.2.18. Deve possuir módulo de proteção contra criptografia maliciosa.
5.7. Smartphones e tablets
5.7.1. Compatibilidade:
5.7.1.1. Dispositivos com os sistemas operacionais:
5.7.1.1.1. Android 5.0 – 5.1.1
5.7.1.1.2. Android 6.0 – 6.0.1
5.7.1.1.3. Android 7.0 – 7.12
5.7.1.1.4. Android 8.0 – 8.1
5.7.1.1.5. Android 9.0
5.7.1.1.6. Android 10.0
5.7.1.1.7. Android 12
5.7.2. Características:
5.7.2.1. Deve prover as seguintes proteções:
5.7.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
5.7.2.1.2. Proteção contra adware e autodialers;
5.7.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;
5.7.2.1.4. Arquivos abertos no smartphone;
5.7.2.1.5. Programas instalados usando a interface do smartphone
5.7.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
5.7.2.2. Deverá isolar em área de quarentena os arquivos infectados;
5.7.2.3. Deverá atualizar as bases de vacinas de modo agendado; 7.2.4.Capacidade de desativar por política:
5.7.2.3.1. Wi-fi;
5.7.2.3.2. Câmera;
5.7.2.3.3. Bluetooth.
5.7.2.4. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
5.7.2.5. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
5.7.2.6. Deverá ter firewall pessoal (Android);
5.7.2.7. Capacidade de tirar fotos quando a senha for inserida incorretamente;
5.7.2.8. Capacidade de enviar comandos remotamente de:
5.7.2.8.1. Localizar;
5.7.2.8.2. Bloquear.
5.7.2.9. Capacidade de detectar Root em dispositivos Android;

5.7.2.10. Capacidade de bloquear o acesso a site por categoria em dispositivos;
5.7.2.11. Capacidade de bloquear o acesso a sites phishing ou maliciosos;
5.7.2.12. Capacidade de configurar White e blacklist de aplicativos;
5.7.2.13. Capacidade de localizar o dispositivo quando necessário;
5.7.2.14. Permitir atualização das definições quando estiver em “roaming”;
5.7.2.15. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
5.7.2.16. Capacidade de agendar uma verificação (Android);
5.7.2.17. Capacidade de enviar URL de instalação por e-mail;
5.7.2.18. Capacidade de fazer a instalação através de um link QRCode;
5.7.2.19. Capacidade de executar as seguintes ações caso a desinfecção falhe (Android):
5.7.2.19.1. Deletar;
5.7.2.19.2. Ignorar;
5.7.2.19.3. Quarentenar;
5.7.2.19.4. Perguntar ao usuário
5.8. Gerenciamento de dispositivos móveis (MDM) - Android
5.8.1. Compatibilidade:
5.8.1.1. Dispositivos com os sistemas operacionais:
5.8.1.1.1. Android 7.0 – 7.12
5.8.1.1.2. Android 8.0 – 8.1
5.8.1.1.3. Android 9.0
5.8.1.1.4. Android 10.0
5.8.1.2. Softwares de gerência de dispositivos:
5.8.1.2.1. VMWare AirWatch 9.3;
5.8.1.2.2. MobileIron 10.0;
5.8.1.2.3. IBM Maas360 10.68;
5.8.1.2.4. Microsoft Intune 1908;
5.8.1.2.5. SOTI MobiControl 14.1.4 (1693);
5.8.2. Características:
5.8.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
5.8.2.2. Capacidade de ajustar as configurações de:
5.8.2.2.1. Sincronização de e-mail;
5.8.2.2.2. Uso de aplicativos;
5.8.2.2.3. Senha do usuário;
5.8.2.2.4. Criptografia de dados;
5.8.2.2.5. Conexão de mídia removível.
5.8.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
5.8.2.4. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
5.8.2.5. Capacidade de desinstalar remotamente o antivírus do dispositivo;
5.8.2.6. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
5.8.2.7. Capacidade de sincronizar com Samsung Knox;
5.9. Gerenciamento de dispositivos móveis (MDM) – iOS
5.9.1. Compatibilidade:
5.9.1.1. Dispositivos com os sistemas operacionais:
5.9.1.1.1. iOS 10.0 – 10.3.3
5.9.1.1.2. iOS 11.0 – 11.3
5.9.1.1.3. iOS 12.0
5.9.1.1.4. iOS 13.0
5.9.2. Características:
5.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
5.9.2.2. Capacidade de ajustar as configurações de:
5.9.2.2.1. Sincronização de e-mail;
5.9.2.2.2. Senha do usuário;
5.9.2.2.3. Criptografia de dados;
5.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
5.9.2.4. Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos clientes através de:
5.9.2.4.1. Link por e-mail;

5.9.2.4.2. Link por mensagem de texto;
5.9.2.4.3. QR Code
5.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS; 9.2.6.Capacidade de, remotamente, bloquear um dispositivo iOS;
5.10. Criptografia
5.10.1. Compatibilidade
5.10.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
5.10.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
5.10.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
5.10.1.4. Microsoft Windows 8 Enterprise x86/x64;
5.10.1.5. Microsoft Windows 8 Pro x86/x64;
5.10.1.6. Microsoft Windows 8.1 Pro x86/x64;
5.10.1.7. Microsoft Windows 8.1 Enterprise x86/x64;
5.10.1.8. Microsoft Windows 10 Enterprise x86/x64;
5.10.1.9. Microsoft Windows 10 Pro x86/x64;
5.10.2. Características
5.10.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;
5.10.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
5.10.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
5.10.2.4. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;
5.10.2.5. Permitir criar vários usuários de autenticação pré-boot;
5.10.2.6. Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real;
5.10.2.7. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
5.10.2.8. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
5.10.2.8.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
5.10.2.8.2. Criptografar todos os arquivos individualmente;
5.10.2.8.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
5.10.2.8.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
5.10.2.9. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente.
5.10.2.10. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
5.10.2.11. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
5.10.2.12. Verifica compatibilidade de hardware antes de aplicar a criptografia;
5.10.2.13. Possibilita estabelecer parâmetros para a senha de criptografia;
5.10.2.14. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
5.10.2.15. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
5.10.2.16. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
5.10.2.17. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
5.10.2.18. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
5.10.2.19. Permite criar um grupo de extensões de arquivos a serem criptografados;
5.10.2.20. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
5.10.2.21. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
5.10.2.22. Capacidade de deletar arquivos de forma segura após a criptografia;
5.10.2.23. Capacidade de criptografar somente o espaço em disco utilizado;

5.10.2.24. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
5.10.2.25. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
5.10.2.26. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
5.10.2.27. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
5.10.2.28. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
5.10.2.29. Capacidade de fazer “Hardware encryption”
5.11. Gerenciamento de Sistemas
5.11.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
5.11.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
5.11.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
5.11.4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
5.11.5. Capacidade de gerenciar licenças de softwares de terceiros;
5.11.6. Capacidade de atualizar informações sobre hardware presente nos relatórios após mudanças de hardware nas máquinas gerenciadas;
5.11.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc);
5.11.8. Possibilita fazer distribuição de software de forma manual e agendada;
5.11.9. Suporta modo de instalação silenciosa;
5.11.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
5.11.11. Possibilita fazer a distribuição através de agentes de atualização;
5.11.12. Utiliza tecnologia multicast para evitar tráfego na rede;
5.11.13. Possibilita criar um inventário centralizado de imagens;
5.11.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
5.11.15. Suporte a WakeOnLan para deploy de imagens;
5.11.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
5.11.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
5.11.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
5.11.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
5.11.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
5.11.21. Permite baixar atualizações para o computador sem efetuar a instalação
5.11.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
5.11.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
5.11.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
5.11.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
5.11.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
5.11.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
5.11.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
5.11.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
5.11.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;
5.12. Instalação e configuração
5.12.1. A CONTRATADA deverá alocar profissionais devidamente certificados pelo respectivo fabricante dos produtos ofertados para fins de execução dos serviços de instalação e de configuração.

5.12.2. As despesas de viagem, hospedagem, alimentação e demais para execução dos serviços correrão integralmente por conta da CONTRATADA;
5.12.3. Caberá ao fabricante disponibilizar, durante todo o período de instalação e configuração, equipe técnica qualificada para esclarecimento de dúvidas, validação das configurações pretendidas e aplicadas, além da resolução de problemas detectados por membros da equipe técnica da CONTRATADA e da CONTRATANTE, sendo que tal equipe poderá prestar os serviços remotamente, quando devidamente aprovada pela CONTRATANTE;
5.12.4. Os serviços de instalação e configuração deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante em seus manuais de configuração ou artigos técnicos;
5.12.5. Os serviços de configuração devem incluir (mas não se limitar a):
5.12.5.1. Criação das tarefas agendadas no servidor centralizado, como atualização de definições de vírus e engine, manutenção da base de dados, replicação para repositórios distribuídos, etc;
5.12.5.2. Criação das tarefas agendadas nos clientes distribuídos, como atualização de definições de vírus e engine, varreduras periódicas, etc;
5.12.5.3. Criação de consultas e relatórios personalizados;
5.12.5.4. Criação das políticas de antivírus e antimalware em geral;
5.12.5.5. Criação das políticas de Device Control;
5.12.5.6. Criação das políticas de agente (quando aplicável);
5.12.5.7. Criação de tarefas automatizadas para sistemas que estão sem a solução de antivírus;
5.12.5.8. Criação da estrutura de árvore hierárquica separadas em níveis de grupos com seus respectivos clientes, tarefas e políticas associadas;
5.12.5.9. Criação de tags personalizadas de categorização de sistemas clientes (quando aplicável);
5.12.5.10. Criação de dashboards gerenciais;
5.12.6. Todos os softwares adquiridos deverão ser instalados nos "datacenters" da CONTRATANTE sob acompanhamento e supervisão da sua equipe técnica.
5.12.7. A CONTRATADA deverá elaborar projeto de implantação (incluindo as atividades de instalação e de configuração) da solução no ambiente tecnológico da CONTRATANTE em conjunto com a respectiva equipe técnica;
5.12.8. A CONTRATADA deverá instalar e configurar todos os softwares das licenças contratada/adquiridas, nas dependências da sede da CONTRATANTE, conforme projeto de implantação por ela elaborado e aprovado pela equipe técnica da CONTRATANTE;
5.12.9. As atividades serão coordenadas e acompanhadas pela equipe técnica da CONTRATANTE;
5.12.10. A critério da CONTRATANTE, os serviços poderão ser executados fora do horário comercial e/ou em finais de semana ou feriados sem custo adicional para a CONTRATANTE, visando minimizar os transtornos aos usuários devido a uma eventual indisponibilidade dos serviços. Por conseguinte, as atividades que não tenham impacto de indisponibilidade poderão ser executadas em horário comercial. Para as atividades que tenham impacto de disponibilidade deverão ser executadas fora do horário de expediente, inclusive em feriados ou finais de semana, de acordo com o for estabelecido entre a CONTRATADA e a CONTRATANTE;
5.12.11. Para todos os efeitos, a conclusão dos serviços de instalação e configuração será atestada pela entrega da solução em pleno funcionamento das licenças ativadas, de acordo com o pacote de serviços adquirido (1, 2 ou 3) e demais condições estabelecidas nesta especificação técnica. Será de responsabilidade da CONTRATANTE, disponibilizar e manter os ATIVOS a serem instalados as licenças da solução.
5.13. Consultoria e suporte técnico.
5.13.1. Caberá a CONTRATADA a prestação dos serviços de consultoria e suporte técnico na Solução de Proteção de Endpoints fornecidos pelo prazo de 36 (trinta e seis) meses, compreendendo suporte telefônico, remoto ou local;
5.13.2. Os serviços de consultoria e suporte técnico a serem prestados não abrangem as atividades referentes à primeira instalação e configuração inicial de cada sistema objeto desta especificação técnica;
5.13.3. Em sua essência, tais serviços visam auxiliar a equipe técnica da CONTRATANTE na administração e na operação do sistema, no âmbito das atividades que exijam conhecimentos com maior grau de complexidade e que possam impactar negativamente no negócio caso sejam executadas sem sucesso;
5.13.4. A CONTRATADA deverá disponibilizar 120 (cento e vinte) horas técnicas de suporte ou de consultoria ao longo da execução do Contrato, podendo estas serem utilizadas a qualquer tempo, mediante solicitação;
5.13.5. Os serviços serão solicitados sob demanda mediante a abertura de chamado efetuada por técnicos da Divisão de Infraestrutura de TIC do TJAM, via chamada telefônica, ou por e-mail, no horário das 9h às 19h (horário de Brasília), de segunda a sexta-feira, informando a modalidade de atendimento no momento da

solicitação;
5.13.6. As horas utilizadas no mês serão enviadas pela CONTRATADA até o dia 10 de cada mês subsequente a finalização do chamado ao Gestor do Contrato da CONTRATANTE para ateste de sua efetiva execução;
5.13.7. Após o recebimento pelo Gestor do Contrato, este terá até 05 (cinco) dias úteis para validação ou questionamento sobre os chamados finalizados;
5.13.8. Após o recebimento do ateste a CONTRATADA deverá emitir a Nota Fiscal para o devido pagamento das horas utilizadas;
5.13.9. As horas técnicas deverão ser prestadas por técnicos devidamente certificados para prestar serviços de consultoria na ferramenta adquirida;
5.13.10. Os serviços de suporte técnico deverão ser prestados observando as seguintes condições:
5.13.10.1. O Suporte Técnico será realizado na modalidade remoto, via telefone, acesso remoto aos equipamentos, mensagem instantânea, Website, e com possibilidade de atendimento on-site na sede da TJAM, para casos em que a CONTRATADA julgar necessário e havendo a concordância da TJAM, no regime de suporte técnico 8x5, com Garantia de Tempo de Resposta (SLA):
5.13.10.1.1. A Garantia de tempo de resposta, será realizada conforme critérios de prioridades abaixo:
5.13.10.1.1.1. Prioridade A — SERVIÇO INDISPONÍVEL: até 8 horas úteis;
5.13.10.1.1.2. Prioridade B — FUNCIONAMENTO PARCIAL: até 24 horas;
5.13.10.1.1.3. Prioridade C — SERVIÇO NORMAL: até 48 horas.
5.13.10.1.2. O suporte remoto deverá contemplar, no mínimo:
5.13.10.1.2.1. Esclarecimento de dúvidas de utilização, administração e operação dos softwares fornecidos e utilizados pelo TJAM;
5.13.10.1.2.2. Poderá ser solicitado o envio de procedimentos para resolver problemas de utilização, administração e operação dos softwares fornecidos e utilizados pelo TJAM;
5.13.10.1.2.3. Fornecer orientação sobre a necessidade de realizar atualização de software para resolver problemas reportados;
5.13.10.2. Os serviços de consultoria e suporte técnico objeto desta contratação compreende, entre outros:
5.13.10.2.1. A análise, elaboração e implantação de projetos que envolvam softwares de antivírus e anti-spyware em uso e os que porventura venham a ser utilizados no TJAM;
5.13.10.2.2. Auxílio na gestão de políticas de segurança da solução CONTRATADA com vistas à prevenção e combate de vírus de computador, spywares - e outras ameaças, sendo desde a avaliação do ambiente atual com ações reativas a emergências e/ou novo projeto com implementação tecnológica atualizada para o mesmo fim;
5.13.10.2.3. Avaliação de vulnerabilidades, prevenção de vírus de computador, spywares e outras ameaças, do ambiente computacional do TJAM;
5.13.10.2.4. A instalação e configuração de atualizações de versões e/ou patches de software;
5.13.10.2.5. A implementação de filtros, políticas, e outros recursos disponíveis na solução de endpoint, a fim de impedir a proliferação de ameaças identificadas e que não disponham, em determinado momento, de vacina;
5.13.10.2.6. O auxílio na auditoria e análise de logs.
5.14. Treinamento
5.14.1. Consiste no fornecimento dos subsídios para que as equipes do TJAM obtenham os conhecimentos adicionais necessários para entender e utilizar as funcionalidades disponibilizadas pela Solução, tais como: arquitetura, configurações, funções e mecanismos de atualização e de distribuição de vacinas e customizações da Solução;
5.14.2. A CONTRATADA deverá fornecer a transferência de conhecimento para os funcionários do TJAM mediante treinamento presencial, com carga horária mínima de 30 horas, que utilize os instrumentos conceituais e didáticos adequados a solução do fabricante da Solução. Deverá ser previsto o treinamento de pelo menos 5 membros das Equipes do TJAM;
5.14.3. O treinamento deverá ser ministrado por profissional com certificação oficial do fabricante da Solução, devendo estes apresentar diplomas e/ou certificações que estejam válidas pelo menos até o último dia da transferência de conhecimento. Estes certificados devem ser encaminhados ao gestor operacional do contrato até o décimo dia útil anterior à data inicial da transferência de conhecimento;
5.14.4. O conteúdo programático do treinamento, bem como as datas e estimativa de tempo para realização do mesma, deverá ser submetido ao gestor operacional do contrato para análise e aceite, devendo compreender no mínimo os seguintes tópicos:
5.14.4.1. Tipos de arquitetura possíveis;
5.14.4.2. Funcionalidades da solução implantada;
5.14.4.3. Implantação e arquitetura do sistema, com opções de expansão e aperfeiçoamento;

5.14.4.4. Utilização avançada do sistema, inclusive com metodologia de criação de políticas;
5.14.4.5. Utilização e customização da solução;
5.14.4.6. Monitoração;
5.14.4.7. Gerenciamento de incidentes;
5.14.4.8. Utilização dos gráficos e relatórios;
5.14.4.9. Interpretação dos gráficos e relatórios.
5.14.4.10. Outros conhecimentos necessários ao entendimento e utilização avançada da Solução, conforme o TJAM e a CONTRATADA julgarem necessário;
5.14.5. Quaisquer custos relativos ao procedimento de treinamento já estão incluídos no valor total deste Pregão;
5.14.6. Esta atividade de treinamento poderá ser realizada pelo fabricante da solução proposta. Todavia, a LICITANTE será a responsável pelo recebimento, gerenciamento e execução de tais demandas, sendo esta LICITANTE o canal de acesso da CONTRATANTE para solicitações desta natureza.

## 6. CARACTERIZAÇAO DO OBJETO

6.1. Os bens a serem adquiridos enquadram-se no conceito de bens comuns, trazidos no parágrafo único do artigo 1º. da Lei nº.10.520/2002.

## 7. QUANTITATIVO

7.1. Para cobrir todos os computadores desktops, máquinas virtuais, servidores e dispositivos móveis do parque computacional com a Solução de Proteção de Endpoints serão necessárias aproximadamente 4000 licenças, um Serviço de Consultoria para instalação e configuração do Servidor, Console Administrativas e Clientes nos Endpoints e um serviço de treinamento para 5 funcionários do TJAM, conforme tabela abaixo:

| Item | Código SIASG/CATMAT | Descrição | Métrica | Unidade | Qtd |
|---|---|---|---|---|---|
| 1 | 369285 | SERVIÇO DE LICENÇAS DE SOFTWARES, Característica(s): especializado em licença de uso do software versão equivalente superior, com suporte e atualizações por 36 meses, Características Adicional(is): conforme Termo de Referência. | Licença | Unidades | 4000 |
| 2 | 20052 | (ID 511957) SERVIÇO DE CAPACITAÇÃO PROFISSIONAL, Característica(s): especializado em treinamento na área de solução de antivírus kaspersky para até 05 (cinco) pessoas, Características Adicional(is): Conforme Projeto Básico/Termo de Referência. | Serviço | Unidades | 1 |
| 3 | 27340 | (ID 511955) SERVIÇO DE CONSULTORIA, Característica(s): especializado em instalação e configuração da solução de proteção para até 4.999 (quatro mil novecentos e noventa e nove) Endpoints, Características Adicional(is): Conforme Projeto Básico/Termo de Referência. | Serviço | Unidades | 1 |
| 4 | 27340 | (ID 515283) SERVIÇO DE CONSULTORIA, Característica(s): especializado em consultoria e suporte técnico por 36 meses na solução de proteção de Endpoints Kaspersky, Características Adicional(is): conforme Projeto Básico/Termo de Referência. | Serviço | Unidades | 120 |

## 8. FORMA DE FORNECIMENTO

8.1. A aquisição das licenças decorrentes deste certame será realizada de acordo com a necessidade e conveniência deste Tribunal, mediante a emissão de requisição de fornecimento e da Nota de Empenho.

## 9. CRONOGRAMA DE EXECUÇÃO

| MÊS | 1 | 2 |
|---|---|---|

| SEMANA | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Elaborar planejamento com CONTRATADA | X | | | | | | | |
| Treinamento | | X | X | | | | | |
| Instalação e configuração de Servidor de Administração e Console Administrativa | | | | X | X | | | |
| Instalação e configuração dos Cliente nos Endpoints | | | | | X | X | | |

**10. SOLICITAÇÃO DE SERVIÇOS**

10.1. A CONTRATADA deverá disponibilizar canais de comunicação telefônica e endereço de correio eletrônico ou plataforma de abertura de chamados para atendimento de suporte técnico e consultoria;
10.2. A CONTRATADA deverá indicar um funcionário para que seja ponto de contato (preposto) entre o TJAM e a CONTRATADA;
10.3. Despesas relativas ao preposto serão de exclusiva responsabilidade da CONTRATADA.

**11. VALOR ESTIMADO**

11.1. Os valores estimados para esta contratação seguem na planilha abaixo.

| Item | Descrição | Unid | Qnt Total | Preço (R$) | |
|---|---|---|---|---|---|
| | | | | Unit | Total |
| 1 | SERVIÇO DE LICENÇAS DE SOFTWARES, Característica(s): especializado em licença de uso do software versão equivalente superior, com suporte e atualizações por 36 meses, Características Adicional(is): conforme Termo de Referência. | Unidades | 4000 | R$ 322,00 | R$ 1.288.000,00 |
| 2 | (ID 511957) SERVIÇO DE CAPACITAÇÃO PROFISSIONAL, Característica(s): especializado em treinamento na área de solução de antivírus kaspersky para até 05 (cinco) pessoas, Características Adicional(is): Conforme Projeto Básico/Termo de Referência. | Unidades | 1 | R$ 95.000,00 | R$ 95.000,00 |
| 3 | (ID 511955) SERVIÇO DE CONSULTORIA, Característica(s): especializado em instalação e configuração da solução de proteção para até 4.999 (quatro mil novecentos e noventa e nove) Endpoints, Características Adicional(is): Conforme Projeto Básico/Termo de Referência. | Unidades | 1 | R$ 38.000,00 | R$ 38.000,00 |
| 4 | (ID 515283) SERVIÇO DE CONSULTORIA, Característica(s): especializado em consultoria e suporte técnico por 36 meses na solução de proteção de Endpoints Kaspersky, Características Adicional(is): conforme Projeto Básico/Termo de Referência. | Unidades | 120 | R$ 12.000,00 | R$ 1.440.000,00 |
| | **Valor Estimado Total** | | | | R$ 2.861.000,00 |

**12. NECESSIDADE DE CONTRATO E VIGÊNCIA**

12.1. Será necessária a formalização de contrato administrativo para a entrega do objeto, devendo ser destacadas as características do objeto, a forma de entrega, obrigações futuras e o valor do mesmo.

**13. PERÍODO DE VIGÊNCIA E REPACTUAÇÃO**

13.1. O Contrato terá vigência de 36 meses a contar de sua assinatura. Os serviços de Suporte, manutenção e garantia terão vigência inicial de 36 meses e, conforme determina o inciso II, do artigo 57 da lei n° 8.666/93, não podendo ser prorrogados.
13.2. As licenças de subscrição de software terão vigência perpétua conforme linha 4.1.3.9. deste Termo.

**14. OBRIGAÇOES E RESPONSABILIDADES DA CONTRATADA**

14.1. Fornecer as soluções, de acordo com as normas legais, verificando sempre o seu bom desempenho, realizando os serviços em conformidade com a proposta apresentada e nas orientações da CONTRATANTE, observando sempre a boa técnica, normas e legislações e os critérios de qualidade dos serviços a serem prestados.
14.2. Prestar todos os esclarecimentos solicitados pela CONTRATANTE de forma clara, concisa e lógica,

cujas reclamações se obrigam prontamente a atender.
14.3. Comunicar ao TJAM, por escrito, qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários.
14.4. Executar os serviços contratados, dentro de elevados padrões de qualidade e obedecendo rigorosamente às condições estabelecidas no Edital.
14.5. A CONTRATADA deve executar o objeto do Contrato conforme Edital e Termo de Referência nos termos das Normas, Portarias, Requisitos Técnicos e demais legislações pertinentes à contratação do objeto em questão, inclusive caberá à CONTRATADA assumir compromisso de cumprir todas as normas relacionadas às questões ambientais quando aplicáveis.
14.6. Providenciar o deslocamento das equipes de trabalho, sem ônus adicional para esta Autarquia, para o atendimento das demandas mencionadas no Termo de Referência.
14.7. Substituir, reparar ou corrigir, em até 05 (cinco) dias úteis, às suas expensas, no todo ou em parte, o objeto deste Termo de Referência em que se verificarem defeitos ou vícios nos uniformes ou na execução, ainda que só detectados quando da sua utilização, arcando com o ônus de serviços rejeitados pela fiscalização que não sejam especificados e/ou considerados mal executados, devendo os mesmos serem refeitos.
14.8. Os danos e prejuízos deverão ser ressarcidos no prazo máximo de 30 (trinta) dias, contados da notificação à CONTRATADA acerca do ato administrativo que lhes fixa o valor, sob pena de multa.
14.9. A CONTRATADA deve cumprir todas as obrigações constantes no Edital, e em seus anexos, conforme oferta final apresentada na sua proposta, assumindo os riscos e as despesas decorrentes da boa e perfeita execução do objeto.
14.10. Manter, durante toda a execução do Contrato, compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação, especialmente, certificação habilitando-a a prestar o respectivo serviço.
14.11. A CONTRATADA deverá facilitar a ação dos Fiscais e do Gestor do Contrato, fornecendo informações ou promovendo acesso à documentação dos serviços em execução, e atendendo prontamente às observações e exigências apresentadas por eles.
14.12. A CONTRATADA deverá atender com presteza às eventuais reclamações sobre a qualidade dos serviços executados, providenciando a sua imediata correção, sem ônus para o CONTRATANTE.
14.13. A CONTRATADA se responsabilizará pela idoneidade e pelo comportamento de seus profissionais, prepostos ou subordinados, respondendo por todos e quaisquer comportamentos e atitudes inadequados de seus profissionais, tais como falta de urbanidade, presteza ou decoro.
14.14. Veda-se à CONTRATADA, sob pena de rescisão e aplicação de qualquer outra penalidade cabível, a divulgação e o fornecimento de dados e informações, referentes à prestação de serviços do objeto dos eventuais Contratos, sem a prévia autorização oficial escrita emitida pelo TJAM.
14.15. A CONTRATADA deverá se responsabilizar pelo cumprimento de toda legislação vigente, incluindo o pagamento de taxas, impostos, emolumentos, multas e demais contribuições fiscais que incidam ou venham a incidir sobre a prestação dos serviços.
14.16. A CONTRATADA deverá atender às despesas e encargos de qualquer natureza com o seu pessoal, necessários à execução do Contrato, responsabilizando-se pelos encargos de natureza trabalhista, previdenciária, fiscal, de acidente de trabalho, e outras.
14.17. A CONTRATADA deverá se responsabilizar pelo ressarcimento de quaisquer danos diretos, comprovados, causados ao órgão ou entidade CONTRATANTE, na execução das obrigações assumidas, respondendo por perdas e danos pela infração cometida ou executada inadequadamente.
14.18. Selecionar e preparar rigorosamente os empregados que irão prestar os serviços, encaminhando, preferencialmente indivíduos portadores de atestado de boa conduta e demais referências, tendo funções profissionais legalmente registradas em suas carteiras de trabalho.
14.19. Fornecer ao CONTRATANTE no início da prestação dos serviços e sempre que houver alteração do quadro de mão de obra, relação nominal dos colaboradores, nela contendo foto, identidade, matrícula, CPF, função e quaisquer outros elementos individuais que comprovem a qualificação do profissional.
14.20. As obrigações decorrentes da licitação constarão de contrato bilateral, fazendo parte integrante do instrumento contratual, guardada a necessária conformidade entre eles, o Edital, a proposta, as especificações e os documentos que os acompanharem.
14.21. A CONTRATADA deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação.
14.22. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Administração.

14.23. Veda-se à CONTRATADA, sob pena de rescisão e aplicação de qualquer outra penalidade cabível, a divulgação e o fornecimento de dados e informações, referentes à prestação de serviços do objeto dos eventuais Contratos, sem a prévia autorização oficial escrita emitida pelo TJAM.

## 15. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

15.1. São obrigações da Contratante:

15.1.1. Realizar os pagamentos devidos à CONTRATADA pela execução dos serviços prestados, nos termos e prazos contratualmente previstos, após a plena verificação de todas as fases merecedoras de fiscalização e da devida aprovação (mensal) por parte do fiscal e do gestor de Contrato.

15.1.2. Proporcionar todas as condições para que a CONTRATADA possa desempenhar os serviços de acordo com as determinações do Contrato, do Edital e deste Termo de Referência.

15.1.3. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.

15.1.4. Notificar a CONTRATADA por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção.

15.1.5. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

15.1.6. Efetuar as retenções tributárias devidas sobre o valor da nota fiscal/fatura fornecida pela CONTRATADA.

15.1.7. Zelar para que durante toda a vigência do contrato sejam mantidas, em compatibilidade com as obrigações assumidas pela CONTRATADA, todas as condições de habilitação e qualificação exigidas na licitação.

15.1.8. Exigir o imediato afastamento de qualquer funcionário ou preposto da CONTRATADA que embarace a fiscalização ou que se conduza de modo inconveniente ou incompatível com o exercício de suas funções.

15.1.9. Rescindir o contrato, pelos motivos por ele aplicáveis, consoante os artigos 77 e 78 da Lei Federal nº. 8.666/1993 nos termos do artigo 80 também daquela Lei.

15.1.10. Quando for o caso, aplicar, à CONTRATADA, as penalidades regulamentares e contratuais cabíveis.

15.1.11. Executar fiscalizações referentes ao serviço prestado pela CONTRATADA, bem como solicitar, quando necessário, documentações imprescindíveis à perfeita execução do contrato.

15.1.12. Auxiliar a CONTRATADA com documentos, informações e demais elementos que eventualmente venham a ser solicitados e que auxiliem nos serviços que tenham a executar.

15.1.13. Exercer fiscalização permanente sobre os serviços executados, objetivando a manutenção de elevado padrão de qualidade dos serviços prestados.

15.1.14. Facilitar o exercício das funções da CONTRATADA, dando-lhe acesso às instalações, promovendo o bom entendimento entre seus funcionários e os empregados do TJAM e cumprindo suas obrigações estabelecidas neste Termo de Referência.

15.1.15. Emitir, com a periodicidade adequada ao objeto fiscalizado, relatório acerca da execução do Contrato, sugerindo, em tempo hábil, as providências necessárias em benefício da Administração.

15.1.16. Ficam reservados ao Gestor do Contrato o direito e a autoridade para resolver todo e qualquer caso singular, omisso ou duvidoso não previsto no processo administrativo e tudo o mais que se relacione com o objeto CONTRATADO, desde que não acarrete ônus para o TJAM ou modificação na contratação.

15.1.17. As decisões que ultrapassarem a competência do Gestor do Contrato deverão ser solicitadas formalmente pela CONTRATADA à autoridade administrativa imediatamente superior ao Gestor, através dele, em tempo hábil para a adoção de medidas convenientes.

15.1.18. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas na execução do objeto, para que sejam sanadas as ocorrências, com as devidas reparações ou correções.

15.1.19. A Administração não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do serviço, bem como por quaisquer danos causados a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

## 16. SUBCONTRATAÇÃO DE SERVIÇOS

16.1. É vedada a subcontratação, cessão ou transferência parcial ou total do objeto do Termo de Referência, sem anuência prévia da CONTRATANTE.

**17. SUPORTE E GARANTIA**

17.1. Garantia e suporte pelo período de 36 (trinta e seis) meses para o objeto deste termo, a contar da data do recebimento dos produtos e serviço.

17.2. Atualizações corretivas e evolutivas de "software", incluindo pequenas atualizações de "release", reparos de pequenos defeitos ("bug fixing" e "patches");

17.3. Suporte técnico especializado para investigar, diagnosticar e resolver incidentes e problemas relativos aos produtos fornecidos;

17.4. Os serviços de garantia e de assistência técnica deverão ser prestados pelo fabricante da solução no regime de 24 (vinte e quatro) horas dia durante os 7 (sete) dias da semana (24 x 7), sem qualquer ônus adicional ao contratante;

17.5. Fornecer consultoria e suporte remoto para os itens deste Termo de Referência.

**18. QUALIFICAÇAO TÉCNICA**

18.1. Atestados de Capacidade Técnica-Operacional

18.1.1. A licitante deverá apresentar no mínimo 1 (um) atestado de capacidade técnica fornecido por pessoa jurídica de Direito Público ou Privado, comprovando que ela forneceu a solução e prestou serviços da mesma natureza deste Termo de Referência e que a solução tenha coberto a quantidade mínima de 4000 Endpoints;

**19. VISTORIA TÉCNICA**

19.1. Não há necessidade de vistoria técnica, pois as instalações físicas, assim como os aspectos de acesso e climáticos, são irrelevantes para o pleno fornecimento da solução objeto deste certame.

**20. LOCAL E PRAZO DE ENTREGA**

20.1. O prazo de execução do objeto será de até 15 (quinze) dias, a contar da data do recebimento da Nota de Empenho;

20.2. A CONTRATANTE será responsável pela definição do local, data e hora de entrega do objeto, conforme necessidade;

20.3. A CONTRATANTE disponibilizará à CONTRATADA, previamente à execução dos serviços objeto do Termo de Referência, todos os controles usados atualmente e que poderão ser melhorados ou substituídos;

**21. DO RECEBIMENTO PROVISÓRIO E DEFINITIVO**

21.1. A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo dos serviços.

21.2. No prazo de até 5 (cinco) dias corridos do adimplemento da parcela, a CONTRATADA deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual;

21.3. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança na execução do objeto, nem ético-profissional pela perfeita execução do objeto, dentro dos limites estabelecidos pela lei ou pelo Contrato.

**22. DO PAGAMENTO**

22.1 O pagamento será efetuado pela Secretaria de Orçamento e Finanças (SECOF) do TJAM, de acordo com a legislação vigente, após recebimento da Nota Fiscal ou Fatura, conferida e atestada pelo setor requisitante, comprovando a prestação do serviço ou o fornecimento do material de maneira satisfatória;

**23. FISCALIZAÇÃO E ACOMPANHAMENTO**

23.1. A fiscalização e o acompanhamento da prestação do serviço será realizada por servidor da Secretaria de Tecnologia da Informação e Comunicação, a ser designado pelo Diretor da Divisão de Infraestrutura de TIC (DVITIC), com as seguintes atribuições:

23.1.1. Acompanhar a execução do contrato, fiscalizando o cumprimento das condições estabelecidas no Termo de Referência, no edital de licitação e na proposta de preço;

23.1.2. Anotar em registro próprio todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados;

23.1.3. Atestar a(s) Nota(s) Fiscal(is) apresentada(s) pela contratada, comprovando a prestação do serviço de

maneira adequada e satisfatória;
23.1.4. Exercer rigoroso controle sobre o cronograma de rotinas de execução dos serviços, aprovando os eventuais ajustes que ocorrerem durante o desenvolvimento dos trabalhos;
23.1.5. Avaliar eventuais acréscimos ou supressões de serviços necessários ao perfeito atendimento do objeto do Contrato, de responsabilidade exclusiva do Gestor;
23.1.6. Aprovar partes, etapas ou a totalidade dos serviços executados, verificar e atestar as respectivas medições, bem como conferir, certificar e encaminhar para pagamento as faturas emitidas pela CONTRATADA;

**24. DA SOLICITAÇÃO DOS SERVIÇOS**
24.1 A solicitação dos serviços se dará através do documento de Ordem de Serviço (OS), em modelo a ser definido oportunamente.
24.2 A prerrogativa de solicitação dos serviços contratados caberá exclusivamente aos seguintes agentes:
24.2.1 Fiscais do Contrato;
24.2.2 Diretor da Divisão de Infraestrutura de TIC;
24.2.3 Secretário de Tecnologia da Informação e Comunicação.

Manaus, data registrada no sistema.

| **Taymon Chris Moura Canté** | **Diogo Mendonça de Sousa** | **Breno Figueiredo Corado** |
|---|---|---|
| Assistente Judiciário - Suporte ao Usuário de Informática | Diretor da Divisão de Infraestrutura de Tecnologia da Informação e Comunicação | Secretário de Tecnologia da Informação e Comunicação |
| *Assinado Digitalmente* | *Assinado Digitalmente* | *Assinado Digitalmente* |

Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO**, **Secretário(a)**, em 22/11/2022, às 08:16, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DIOGO MENDONCA DE SOUSA**, **Diretor(a)**, em 22/11/2022, às 08:36, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **TAYMON CANTE**, **Servidor**, em 22/11/2022, às 09:17, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0806178** e o código CRC **B4B1C2BC**.